SANSlide
SSiS100
iSCSI Node
User Manual
V1.2

Bridgeworks
135 Somerford Road, Christchurch,
Dorset BH23 3PY
Tel: +44 (0) 1202 588 588
Fax: +44 (0) 1202 588 589
Email: support@4bridgeworks.com

Manual Revision History

Revision	Date	Firmware	
1.0	April 2012	V3_02	AP
1.1	August 2012	V3_02	AP
1.2	October 2013	V3_04	AP

Warning

The Bridgeworks SANSlide Node contains no user serviceable components. Only an authorised service centre should carry out servicing or repairs. Unauthorised repairs or modifications will immediately void your warranty.

Before you start

There are a number of additional pieces of equipment you will require for the successful installation of your Node:

Ethernet Cable

You will require a good quality cable of suitable length to go between your network access point and the iSCSI Node. This should be marked as certified to Cat 5e and have a RJ45 style connector at the Node end.

If you are in any doubt contact your reseller for extra assistance.

Table of Contents

1.0 Introduction

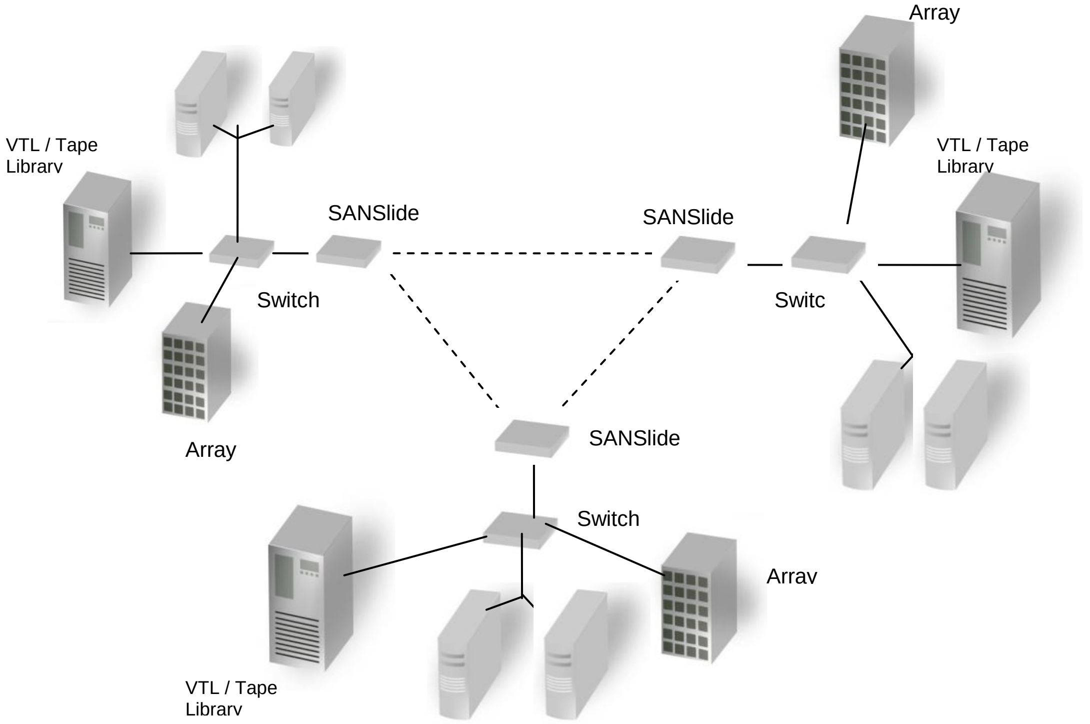
Thank you for purchasing the Bridgeworks SANSlide Node.

Bridgeworks have designed the SANSlide product to be intuitive and easy to install and configure. However, we would recommend that you work in conjunction with this manual when you first configure the SANSlide Node.

1.1 Overview

The SANSlide product range has been designed to connect storage devices over long distance, high latency TCP/IP networks with very little loss in performance. It supports all the major storage protocols such as Parallel SCSI, Fibre Channel, iSCSI and SAS. More interfaces will be added, as they become part of the mainstream storage protocols.

A SANSlide installation consists of a number of Nodes connected via a TCP/IP network as shown below.



Example SANSlide Installation

Each Node’s storage interface can be configured to act either as a target interface – working in a similar mode to a storage device, or as an initiator – working in a similar mode to a server. Or, if the SANSlide Node has multiple storage interfaces, one can be configured to be an initiator and one as a target device.

A unique part of SANSlide functionality is that all the Nodes within a SANSlide installation do not have to have the same storage interface. Therefore, it is quite feasible to have the data centre Node connected to a Fibre Channel network whilst a remote Tape Library is connected via a parallel SCSI Node.

1.2 Manual Layout

This Manual has been divided into two primary sections an installation guide, and a more detailed section containing all of the functionality available to you, which is divided into sections that correspond to the web interface.

Throughout the manual symbols will be used to quickly identify different pieces of information.

✎	This icon represents a note of interest about a step or section of information.

☞	This icon represents an important piece of information.

⚠	This icon represents a warning, care must be taken and the warning should be read thoroughly.

1.3 Definitions

Throughout this manual selected terms will be used to describe pieces of equipment and concepts. Below is an explanation of those terms.

- Node – A Node refers to the physical SANSlide unit you have purchased.

- Target Device – A disk or tape drive connected to a SANSlide Node each device is identified by an IQN – iSCSI Qualified Name

- Initiating Device – A computer or other piece of equipment, which can perform backups connected to a SANSlide Node via iSCSI.

- Initiator Node – A Node which has both of its' ports configured to be Initiators.

- Target Node – A Node which has both of its' ports configured to be Targets.

- Remote Node – A Node, which has at least one initiating Port, which has, or is intended to have, a target device connected to it.

- Local Node - A Node, which has at least one Target Port, which has, or is intended to have, an initiating device connected to it.

2.0 Hardware Installation

The first step to configuring your Nodes is to set up the hardware, It is recommended that if you are going to follow the installation guide that you first plug your hardware in at an easily accessible test area before adding it to cabinets or shipping the remote board to your offsite location.

2.1 Ethernet Connection

The Node can be used on the following network configurations:

- 10BaseT
- 100BaseT
- 1000BaseT (Gigabit)

It is not necessary to specify which network type you are connected to, as when powered up the Node will automatically select the correct network speed.

The connection to the Ethernet network is via an industry standard twisted pair, RJ45 copper interface on the front of the unit.

To connect the Node to the Ethernet network, insert two Cat 5E cables into the connector on the unit as shown below. When the plug is in the correct position a “click” should be heard.

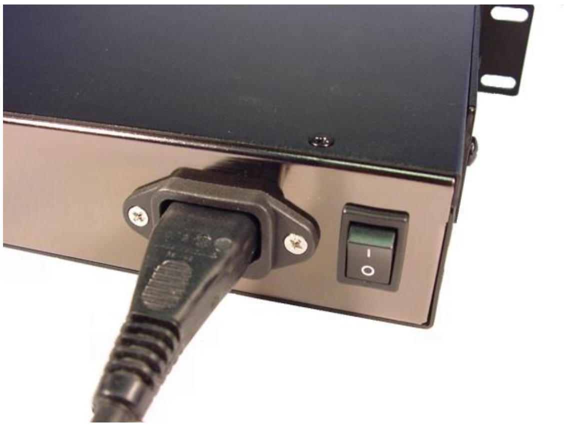
✎	**Note:** SANSlide requires both Ethernet ports to be connected to the network. The left hand port is used to access the Node manager, the right hand port is used for the SANSlide connection.

Front Panel of the Node Showing Ethernet Cable Connections

2.2 Connecting the Power Supply

Before connecting the Power Supply to the unit, ensure the wall plug is removed or switched off.

Connect the Power Supply to the rear of the Node as shown below.



✎	**Note:** Before powering up the Node, ensure all the peripherals are powered up and you have a connection to the network.

To turn on the Node use the switch next to the power connector and push in the button. (The image above shows the button in the off position). Whenever the Node is powered on the blue LED on the front panel will be illuminated.

Now that the Node is installed, the next stage is to configure it. This is described in the next chapter.

3.0 Using the Web Interface

Now the SANSlide Node is fully connected the primary method for configuring any option is through its web interface. The following section highlights the requirements needed to access these pages and the consistent layout used throughout.

Note: The default IP address of the web interface for the Node is **http://10.10.10.10/**

3.1 Browsers

This Node supports the following browsers

- Microsoft Internet Explorer 6
- Microsoft Internet Explorer 7
- Microsoft Internet Explorer 8
- Mozilla Firefox 2
- Mozilla Firefox 3

Note: JavaScript must be enabled within the web browser to use the web interface's functionality.

☞ **Important:** If you choose to use a browser that is not on the list of supported browsers Bridgeworks cannot guarantee the behaviour of the Node's functionality.

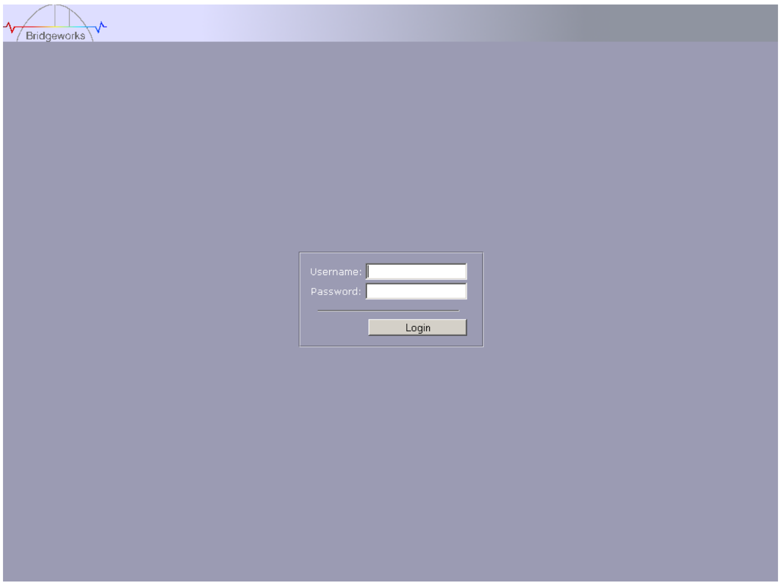
3.2 Connecting to the Web Interface

From within your web browser, connect to the Node using the address http://10.10.10.10/ (or if you have changed this previously, the address of the left-hand network port from the bottom two).

Note: By default, all Nodes have the same IP address and Hostname. Bridgeworks strongly recommend that you complete the network configuration of your Nodes, one Node at a time to avoid any confusion.

Depending on your current network parameters, it may be necessary to change your network setting on your computer for the initial set up. See Appendix A for further help.

Once you have connected to the GUI on the Node you will see the entry page shown below.



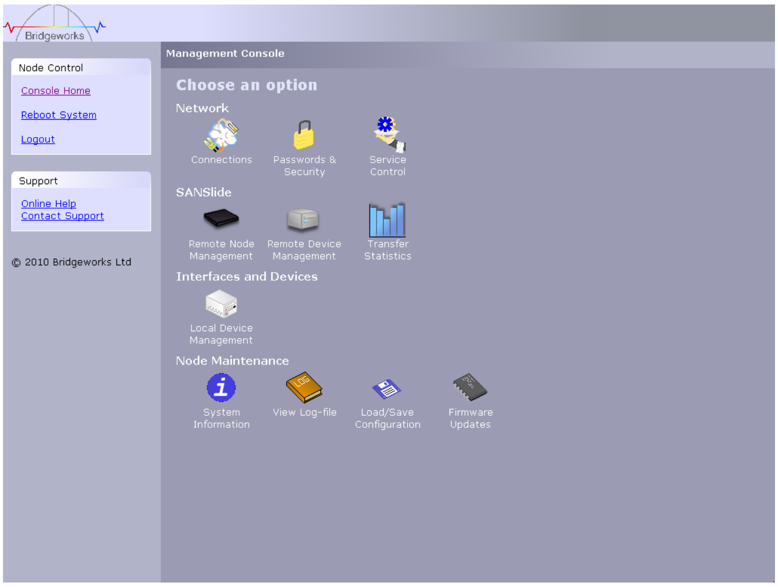
SANSlide Node Login

To access the web interface a user name and password must be used, the default of which are:

- Username: **admin**
- Password: **admin**

3.3 Management Console

The GUI will now display the root selection screen as shown below.



SANSlide Node main menu

Note: Your screen may have different icons to the one shown above depending on the configuration you have purchased

You will notice the screen is split into two sections. Within the left hand panel you will observe two further panels. The upper panel "Node Control" typically remains constant wherever you are within the GUI, it allows you to reboot or logout of the GUI whilst the console home link will take you back to this screen.

Note: Whenever a Reboot command is issued it can take up to a minute for the Node to become accessible again.

Within the Support section there is a link that will open up your mail service with Bridgeworks' Email address loaded and an Online Help button. The Online help is contextually aware of which GUI page you are currently viewing and will provide you with help relevant to the display and configuration data.

4.0 Installation Set Up

To avoid travelling between sites where the Nodes are installed, Bridgeworks has included a feature within the GUI making it is possible to connect to and manage, a remote Node from another Node. However, to achieve this, the IP address of the remote Nodes WAN port must be known, therefore, the steps are divided into two sections:

- Local Configuration: these steps are preformed with you having direct access to both Nodes.

- Installed Configuration: these steps are preformed with one of the Nodes being configured in a remote location.

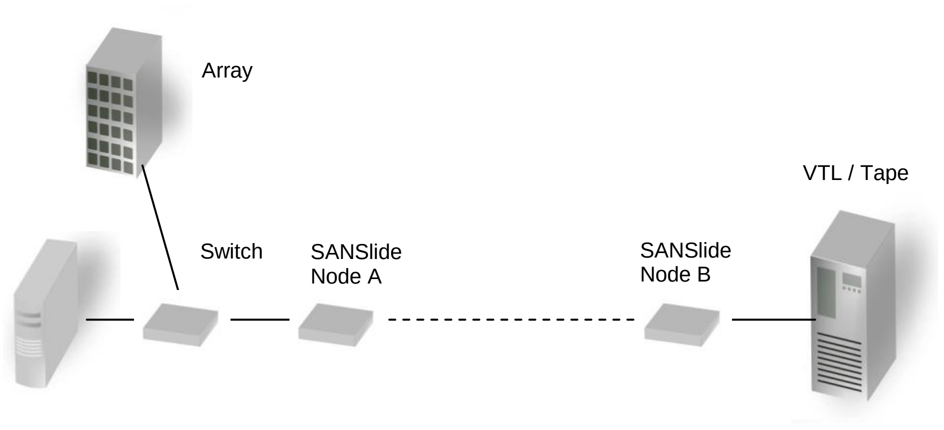
If at any point during the installation guide a mistake is made, or you become worried about the configuration you have entered, the Node can be restored back to factory defaults and the process can be started again, see the section 8.5 Restore to Factory Defaults.

4.1 Example Configurations

The following examples will be used throughout the rest of the Installation guide. If an example Node is not specifically referred to then that step is to be applied to both sets of example boards. It is recommended you choose the example that matches your requirements and follow the instructions provided.

Example 1: Remote tape libraries

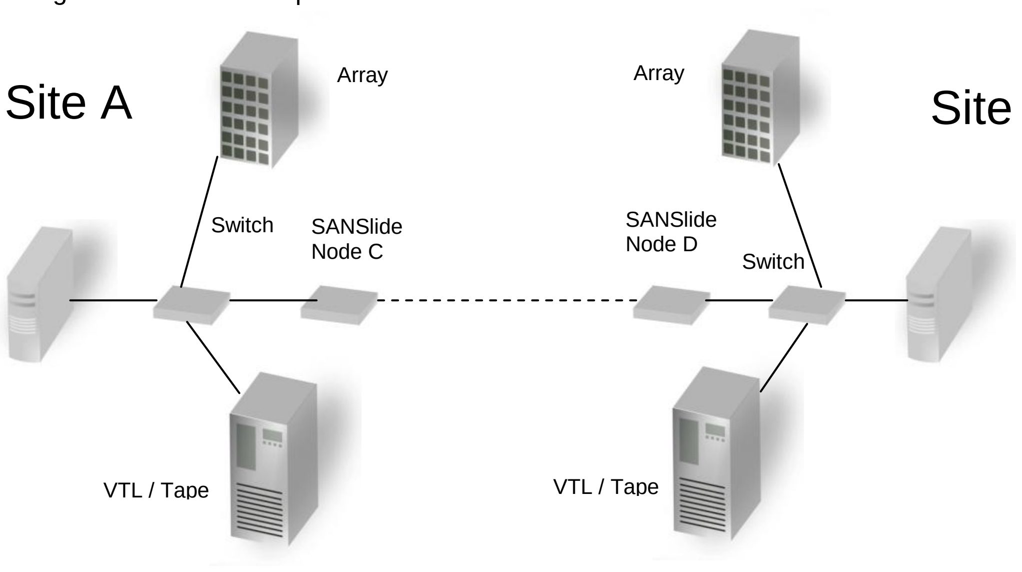
Here we have a Server based in the data centre and an iSCSI enabled Tape Library in a remote location. The SANSlide Node A in the data centre is configured to be a Target Node, whilst the SANSlide Node B in the remote location is configured to be an Initiator Node.



Remote Tape Libraries

Example 2: Across-site back up

Here we have servers in both data centres backing up to a tape library located in the other data centre. In this case one interface on each Node C and D is configured to be a target port whilst the other interface is configured as an Initiator port.



Across Site back-up

4.2 Local Configuration

This section will take you through the steps required to configure the SANSlide Nodes so they can communicate with each other before connecting them to the storage networks and the link network. The local configuration will take you through the following steps:

- Step 1: Configuring Network Connections
- Step 2: Testing the Connection
- Step 3: Security Options (Optional)
- Step 4: Linking together SANSlide Nodes

Once these steps have been repeated for all your Nodes, the Nodes can be moved to their permanent respective positions.

Step 1: Configuring Network Connections

The following steps will configure the networking options for your Nodes and should be completed for Example 1: **Nodes A** and **B** or Example 2: **Nodes C** and **D**.

Basic Information

The Node has two GbE (Gigabit Ethernet) Network ports located on the front of the unit. The left hand port is used to access the Node Management Console, the right hand port is used for the SANSlide link.

There are two possibilities when configuring the IP addresses of the Node. Management A can be configured in one of two ways:

- DHCP - The Node will seek out the DHCP server on your network and obtain an IP address from the server each time it powers up. With this option when accessing the web interface the host name will be entered into the web browser.

- Static IP - the IP address set in this page will be the IP address the unit will use each time it powers up. Network port two is the SANSlide connection and it must have a static IP address.

It is recommended that static address be used for the iSCSI links and the SANSlide links,

Note: If you select the DHCP mode, Bridgeworks recommends you ensure your DHCP server is set to automatically update the DNS server.

Before You Begin

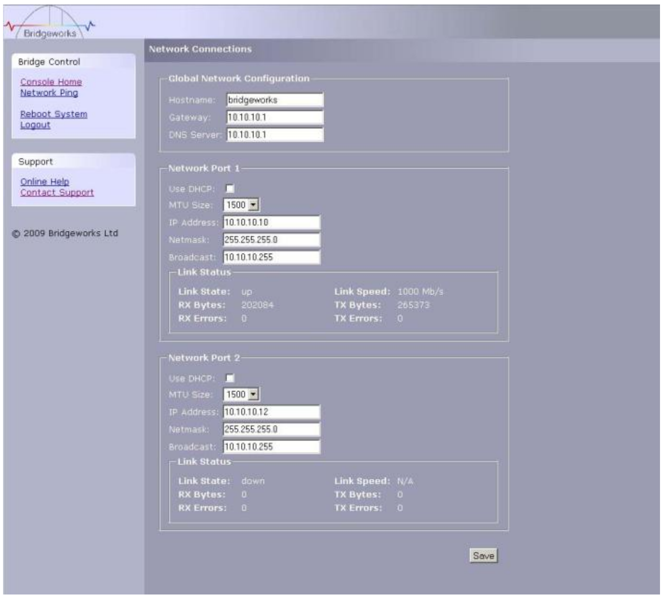
Depending on your current network parameters, it may be necessary to change your network setting on your computer for the initial set up. See Appendix A for further help.

Note: By default, all Nodes have the same IP addresses and Hostnames.

Ensure that these settings are unique to each Node.

Navigation

Click on the “Connections” button under the Network section of the main window. This will now bring up a new configuration page as shown below.



Network Connections

Global Network Configuration

Hostname: bridgeworks
Gateway: 10.10.10.1
DNS Server: 10.10.10.1

Network Port 1

Use DHCP: □
MTU Size: 1500
IP Address: 10.10.10.10
Netmask: 255.255.255.0
Broadcast: 10.10.10.255

Link Status

Link State:	up	Link Speed:	1000 Mb/s
RX Bytes:	202084	TX Bytes:	265373
RX Errors:	0	TX Errors:	0

Network Port 2

Use DHCP: □
MTU Size: 1500
IP Address: 10.10.10.12
Netmask: 255.255.255.0
Broadcast: 10.10.10.255

Link Status

Link State:	down	Link Speed:	N/A
RX Bytes:	0	TX Bytes:	0
RX Errors:	0	TX Errors:	0

Network Connections

Procedure: Configuring network ports

Steps:	1.1: Enter in the Hostname field the name you wish to use to address this Node in the future. It is recommended that you use a name that is relevant to its location and/or its' purpose. 1.2: Enter in the IP address you have chosen or select DHCP for network port 1. Network port 2 is used for the SANSlide connection and must have a static IP address. 1.3: If the Node is configured to use DHCP the net mask will be issued from the DHCP server. If you are using a static IP address, enter the net mask in to this box. This must be done for any network port not using DHCP. 1.4: Click the save button to save these parameters and then click the reboot option under "Node Control" in the left hand pane. 1.5: To reconnect to the Node you will need to use the new Hostname or IP address for network port1, depending on which addressing mode you have selected. 1.6: Repeat step 1.1 to 1.5 for any additional Nodes and network ports you wish to configure.

	Note: None of these changes will take effect until a reboot is completed.

Result

When you next login to the web GUI you should now have to use your new network address.

Related Topics

- 5.1 Connections
- 9.2 Lost IP Address

Step 2: Testing the Connection

The following steps will verify your chosen network connections and should be completed for Example 1: **Nodes A** and **B** or Example 2: **Nodes C** and **D**.

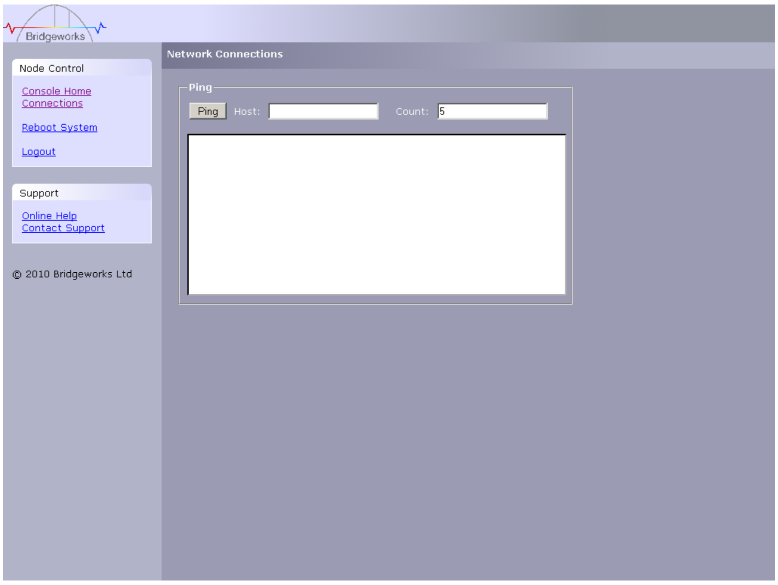
Before You Begin

If you made changes to your computer, return them to their previous setting and reconnect to the Node using the IP address or hostname, depending on which addressing mode you selected.

You will need to have to hand at least two Cat5e or better network cables.

Navigation

Select the Connections page from the root page and at the top of the left-hand column in “Node Control” you will find a link to the ping window called “Network Ping”. Select this link. The GUI will display the following screen.



Count: 5

Network Ping

Procedure: Testing the connection between Nodes

Steps:	2.1: Connect the Nodes together using network port two; the Node will automatically detect the cable type so either a crossover or straight through cable can be used. 2.2: Enter in the IP address of network port two from the other Node (the Node you are not currently accessing the Web interface from, for example if you are connected to Node A enter in the address of network port two on Node B) and click ping.

Result

On a successful ping the text box below the buttons should fill with text similar to that below

```
PING Address (Address): 56 data bytes
64 bytes from Address: seq=0 ttl=64 time=0.600 ms
64 bytes from Address: seq=1 ttl=64 time=0.129 ms
64 bytes from Address: seq=2 ttl=64 time=0.096 ms
64 bytes from Address: seq=3 ttl=64 time=0.143 ms
64 bytes from Address: seq=4 ttl=64 time=0.094 ms

--- Address ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.094/0.212/0.600 ms
```

✎	**Note:** Where “Address” is the IP address you entered.

If the results of the ping match the output above this completes the initial set up, if not please retry step 1.

Related Topics

- 5.1 Connections

Step 3: Security Options (Optional)

You will only need to complete this step if:

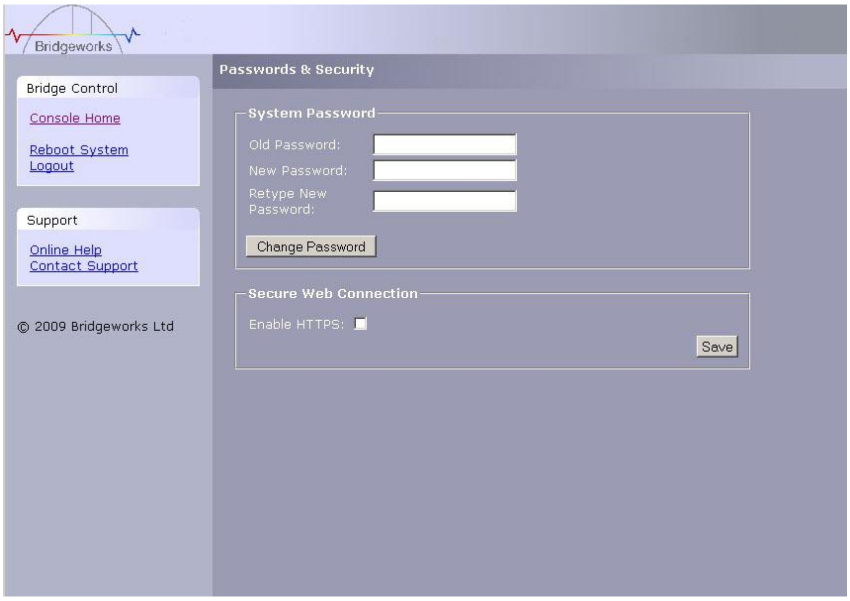
- You want to change the password from the default.
- You want to enable HTTPS.

This stage is not necessary for configuring the Nodes but for your security it is recommended to complete the following configuration changes. If you do not require these features or are going to configure them at a later stage proceed to step 4.

The following can be completed for Example 1: **Nodes A** and **B** or Example 2: **Nodes C** and **D**.

Navigation

Click on the “Passwords & Security” button under the Network section of the main window. This will now bring up a new configuration page.



Passwords and Security

Procedure: Changing the Admin password and enabling HTTPS

Steps:	3.1: Click the checkbox next to Enable HTTPS and click on save. A pop up message will inform you that you are going to be logged out, click “OK”. 3.2: Login to the Node again under HTTPS. 3.3: Navigate back to the “Passwords & Security” page. 3.4: Enter your existing password; the default is **“admin”** in the old password field. 3.5: Enter the new password of your choosing into the new password field. 3.6: Re-enter the new password of your choosing into the “Retype New Password” field.

Result

You are now using HTTPS within your browser; this can be verified by confirming the web address starts with https://. Depending on your browser or if you have completed these steps before, it may become necessary to accept a security certificate or specify to ignore an invalid certificate.

Once the password has been changed successfully the message “Password successfully changed” will appear.

Related Topics

- 5.2 Passwords & Security

Step 4: Linking together the SANSlide Nodes

The following steps will link together your Nodes and should be completed for Example 1: **Nodes A** and **B** or Example 2: **Nodes C** and **D**.

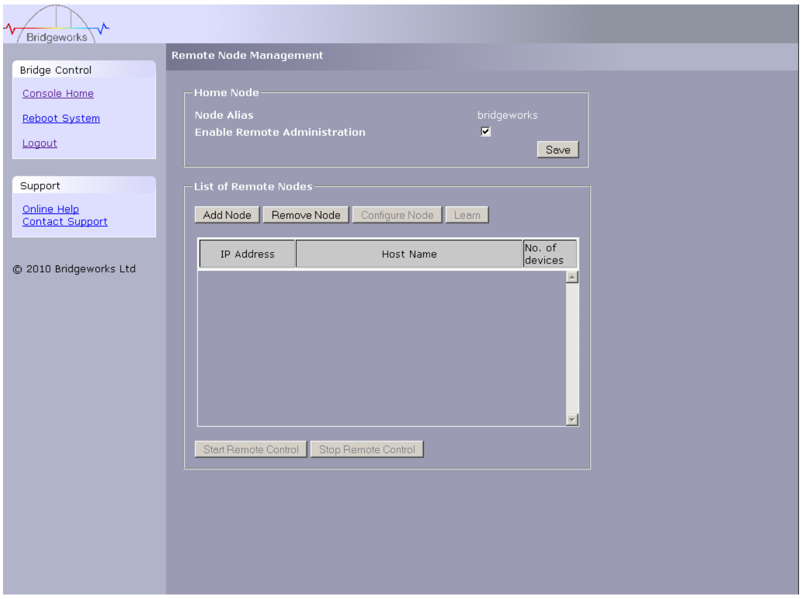
Basic Information

The IP address used to discover the Node is the address you have assigned to the WAN port on the Node you want to add.

SANSlide will always attempt to get the best performance possible for the data it is transferring, however there may be other traffic on your network that will also need to accesses a share of your links bandwidth, this is where the configuring of a SANSlide Node comes in.

Navigation

From within the root window select the Remote Node Management icon. The following screen will be displayed.



Node Alias: bridgeworks

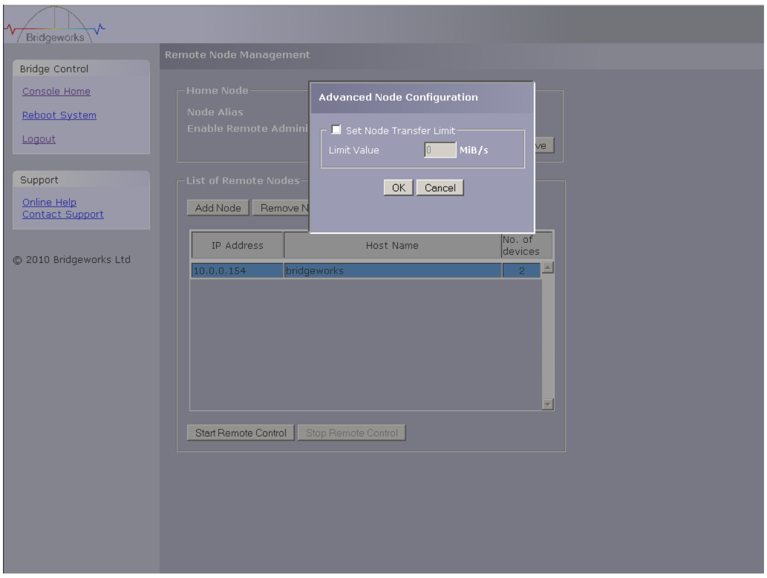
Enable Remote Administration ☑

Remote Node Management

Procedure: Adding a SANSlide Node

Steps:	4.1: Click on the “Add Node” button 4.2: In the window that appears, enter the IP address then click the Add button. The unit will then search for the Node on the Link Network, as indicated by a blue progressing bar. 4.3: Click on “Ok” to confirm the Node. 4.4: If you have more than one Node, repeat this operation for all Remote Nodes.

	Note: These Nodes will be automatically saved, and will restore on reboot.



IP Address	Host Name	No. of devices
10.0.0.154	bridgeworks	2

Configuring a Node

These steps are only necessary if you want to limit the amount of bandwidth SANSlide uses.

Procedure: Limiting bandwidth

Steps:	4.1: Select a Node from the Node list, when selected the background colour will become blue. 4.2: In the window that appears check the “Set Transfer Limit checkbox”. 4.3: Enter in the limiting value in Megabytes a second. 4.4: Click on “Ok” to start the limit.

	Note: The bandwidth limit will become instantly effective.

Result

The Remote Node(s) you have added will be displayed in the “List of Remote Nodes” list.

Related Topics

- 6.1 Remote Node Management

4.3 Installed Configuration

Now you have completed the local configuration, the Nodes can now be relocated to their remote locations and the continuation of the configuration can be done remotely.

The Installed Configuration will take you through the following steps:

- Step 5: Remotely Connecting to a Node (Optional)
- Step 6: Configuring the iSCSI Initiator
- Step 7: Configuring the iSCSI Target (Optional)
- Step 8: Refreshing the Devices
- Step 9: iSCSI Sessions (Optional)
- Step 10: Instigating the Learn Process

Step 5: Remotely Connecting to a Node (Optional)

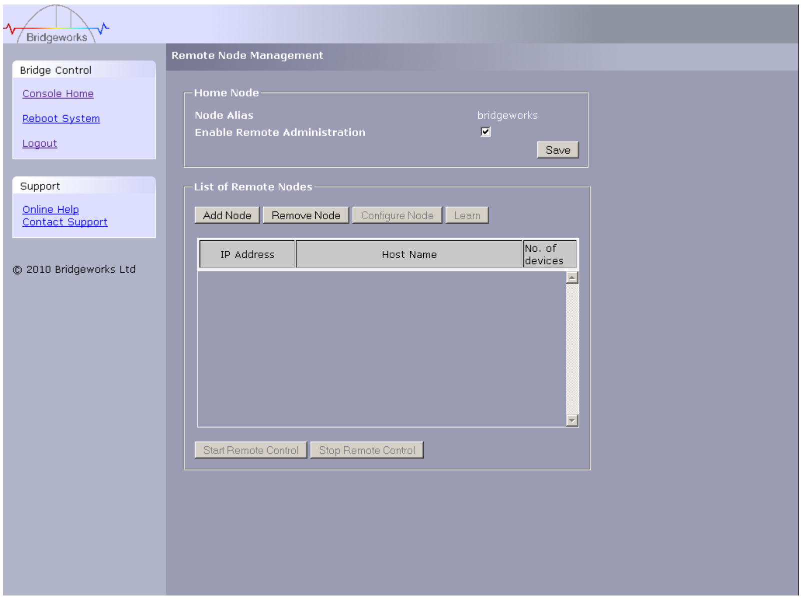
You will only need to complete this step if:

- You want to configure the settings on a Node and do not have direct access to the web interface for that Node.

During the set up of your Nodes it may not be possible to directly access the web interface on a Node, “remote control” can be used to take control of any other Node added to your local Node.

Navigation

From within the root window select the Remote Node Management icon. The following screen will be displayed.



Node Alias: bridgeworks

Enable Remote Administration ☑

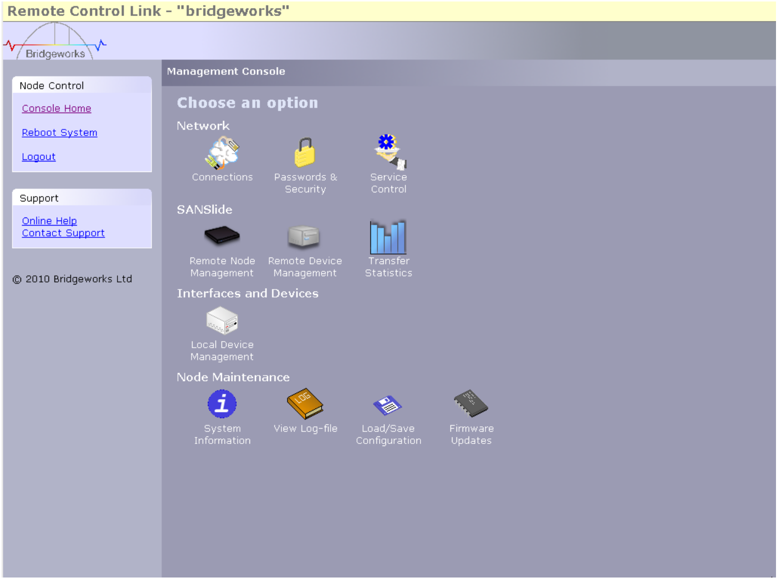
Remote Node Management

Procedure: Starting remote Node control

Steps:	5.1: Highlight the Node you wish to connect to by clicking the Node in the remote Node list. 5.2: Click the Start Remote Node Control button at the bottom of the list. 5.3: The Web Interface will now display the login screen of the remote Node as normal, login to that Node using the credentials of the remote Node. 5.4: Repeat this process with any other Nodes you may have to configure.

Result

Whenever a remote control session is underway there will be a yellow bar at the top of the web interface which will contain the name of the Node you are connected to, as illustrated below.



A remote Node under remote control

Related Topics

- 6.1 Remote Node Management

Step 6: Configuring the iSCSI Initiator

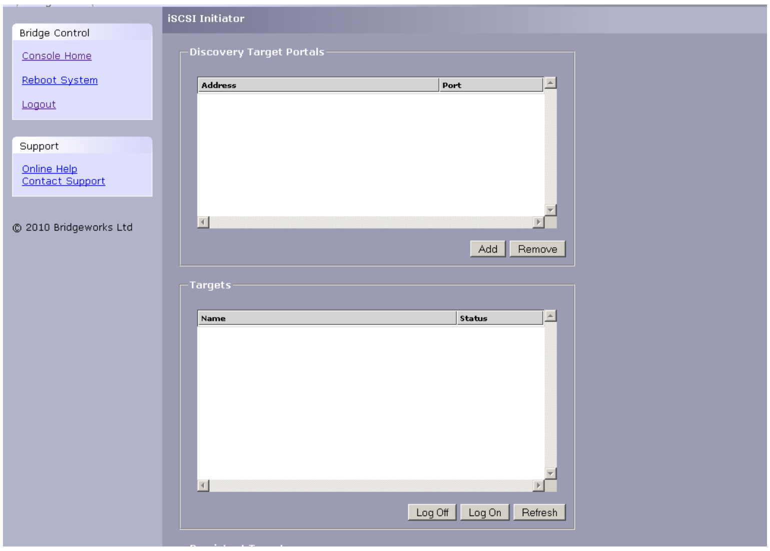
The following steps will discover and log into your chosen target devices, the steps should be completed for Example 1: **Nodes A** or Example 2: **Nodes C** and **D**.

Information

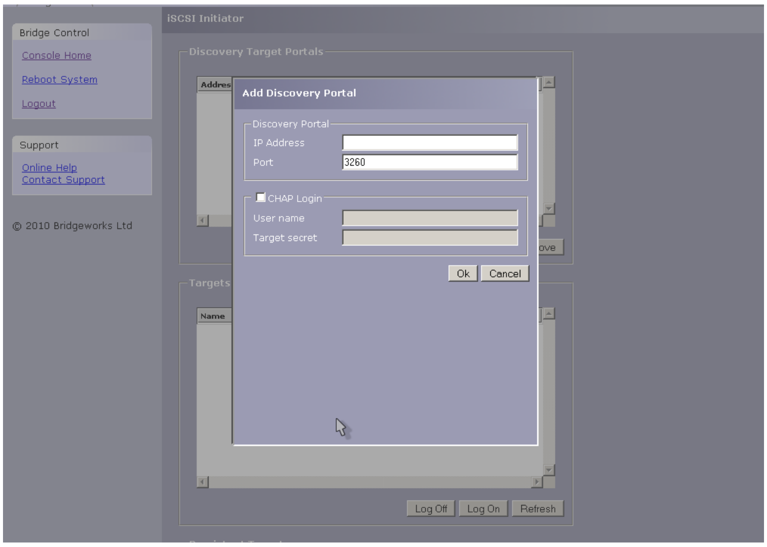
An iSCSI target device is device such as a disk drive, tape drive or RAID controller that is attached to the network. Each device is identified by an iSCSI Qualified Name (IQN). Anything connected to a network, be it a computer, printer or iSCSI device must have a unique identifier, such as an IP address, to enable other devices to communicate with it. With iSCSI devices (both targets and initiators) an extra level of identification in addition to the IP address is employed, called the IQN. The IQN includes the iSCSI Target's name and an identifier for the shared iSCSI device.

Navigation

Select the iSCSI Initiator icon from the root menu. GUI will display the following screen.



iSCSI Initiator Configuration



iSCSI Addition of a discovery portal

Procedure: Discovering iSCSI targets

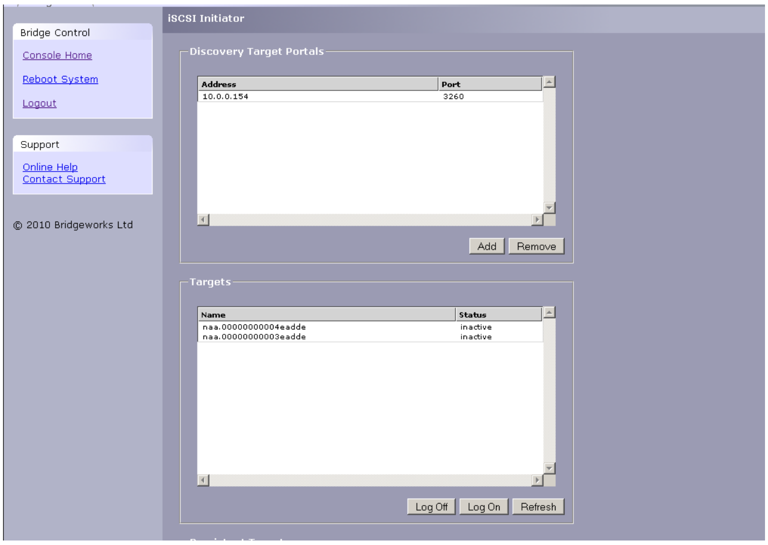
Steps:	6.1: Click on the Add button, a pop up menu will appear. 6.2: Under discovery portal enter in the IP address the iSCSI device is connected to. 6.3: (Optional) Enter in the TCP port number, it is recommended to leave it at the default value unless necessary.

	Note: The default port number for iSCSI is 3260, unless you have specifically changed this it is recommended to leave it at the default values.

The following steps are optional if you have set up any CHAP credentials. If not progress to step 6.10.

Procedure: Setting CHAP credentials

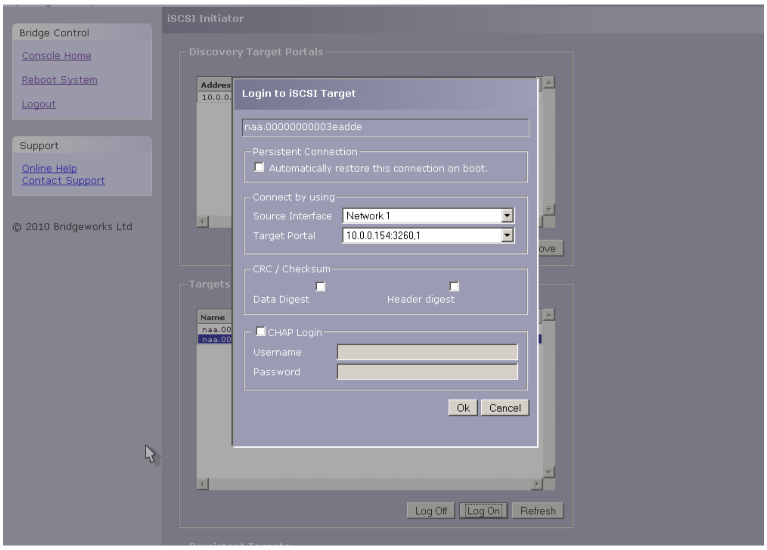
Steps:	6.4: Click the CHAP login checkbox 6.5: Enter in the username for the chap login 6.6: Enter in the password for the chap login 6.7: Click OK 6.8: When successful, the discovery will then be added to the Discovery Target Portals. 6.9: Repeat from step 6.1 for each additional IP address you have targets connected to, if there are discovery portals to add progress to the next step.



Address	Port
10.0.0.154	3260

Name	Status
naa.00000000004eadde	inactive
naa.00000000003eadde	inactive

iSCSI Discovery with two target devices discovered



Login to iSCSI Target

naa.00000000003eadde

Persistent Connection

□ Automatically restore this connection on boot.

Connect by using

Source Interface: Network 1

Target Portal: 10.0.0.154:3260,1

CRC / Checksum

□ Data Digest □ Header digest

□ CHAP Login

Username:

Password:

iSCSI target logging on.

Procedure: Logging on to Targets

Steps:	6.10: Select a target from the Targets list, each target is displayed by its IQN, when selected the background colour will become blue. 6.11: Click the Log On button underneath the list, a pop up menu will appear. 6.12: If you wish for the unit to connect to this IQN after a reset or reboot, then check the “Automatically restore this connection on boot” checkbox. It is recommended that this feature be enabled. 6.13: Select the source interface, this is the physical network port that your device is connected on. 6.14: Select the target portal from the drop down menu; the target portal reflects the network interface and the port that the target device is connected on. 6.15: If you wish for data correction and checksums to be used select, either or both of the checkboxes Data Digest or Header Digest.

✎	**Note:** CRC/Checksum settings allow you to specify whether data transfer is done using Data and/or Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended that Header and Data Digests are left disabled, as performance will be affected.

The following steps are optional if you have set up any chap credentials. If not progress to step 6.19.

Procedure: CHAP Login

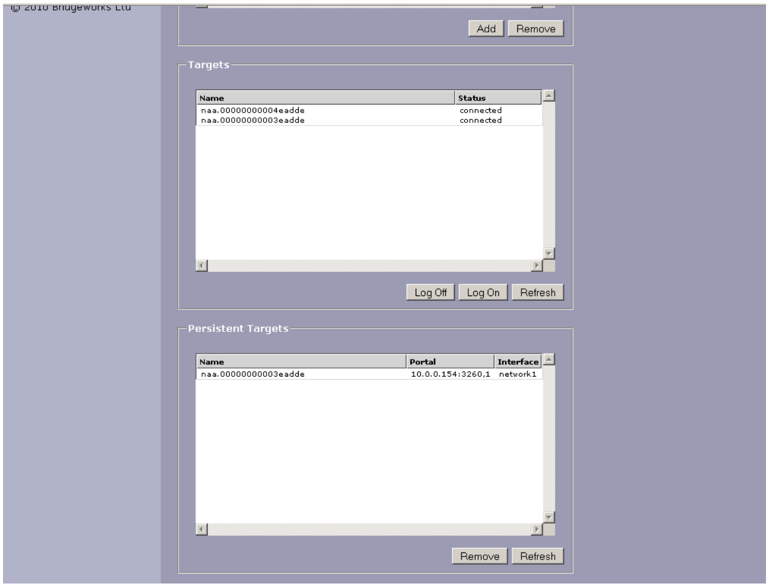
Steps:	6.16: Click the CHAP login checkbox 6.17: Enter in the username for the CHAP login 6.18: Enter in the password for the CHAP login 6.19: Click OK

6.20: The status will now change from inactive to active within the targets table.

6.21: Repeat from step 6.11 for each additional target you want to logon to, if there are no more progress to the next step.

6.22: Repeat from step 6.1 for Example 2: Node D, or if you have completed the procedure for all required Node sets precede to the next step

Note: Any targets that you selected to be persistent will now be present in the persistent targets list.



Name	Status
naa.00000000004eadde	connected
naa.00000000003eadde	connected

Name	Portal	Interface
naa.00000000003eadde	10.0.0.154:3260,1	network1

Successful addition of persistent targets

Result

Every target has been successfully logged into the local Node.

Related Topics

- 7.2 Configuring and Connecting iSCSI Devices
- Appendix E LED Indicators

Step 7: Configure the iSCSI Target (Optional)

You will only need to complete this step if:

- You want to add CHAP authentication credentials.
- You want to change the TCP port number iSCSI connects on.

If you don't require changing these settings skip to the next step.

The following Nodes Example 1: **Node B** and Example 2: **Node C**, **Node D** are the only Nodes that may require the following steps.

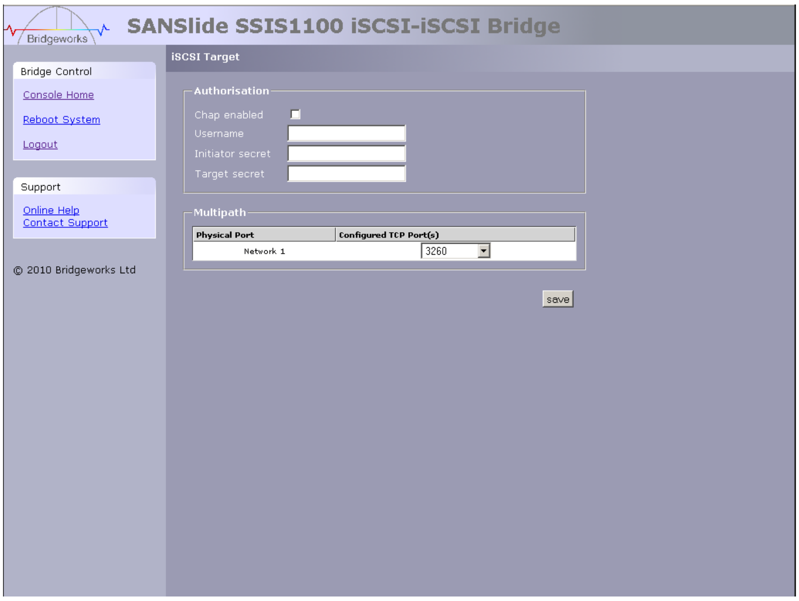
Information

CHAP is an authentication scheme used by servers to validate the identity of clients and vice versa. When CHAP is enabled, the initiator must send the correct username and Target password to gain access to the iSCSI Node. The Initiator secret is provided to allow iSCSI mutual CHAP. If mutual CHAP is selected on the Initiator, the iSCSI Node will authenticate itself with the initiator using the initiator secret

If you wish to perform mutual authentication (after the iSCSI Target has authenticated the iSCSI initiator, the iSCSI initiator will authenticate the iSCSI Target) - the iSCSI initiator secret field will have to be filled.

Navigation

From the root menu select the iSCSI target icon, the GUI will display the following screen.



SANSlide SSIS1100 iSCSI-iSCSI Bridge

iSCSI Target

Authorisation

Chap enabled □
Username
Initiator secret
Target secret

Multipath

Physical Port	Configured TCP Port(s)
Network 1	3260

iSCSI Target

Procedure: Enabling CHAP

Steps:	7.1: Enable the CHAP enabled checkbox. 7.2: Enter in your chosen username. 7.3: Enter in the initiator secret if you are choosing to use mutual chap, this is the

	password defined in the iSCSI host 7.4: Enter in the Target secret; this is the password that the Node will send to the iSCSI host. 7.5: Click on the save button, the changes will take effect immediately.

✎	**Note:** The initiator and target passwords must be between 12 and 16 characters in length and must be unique to each other.

Procedure: Changing the listening port

Steps:	7.6: From the table, Select the TCP port number from the drop down list, next to the network port number you wish to change. 7.7: Repeat step 7.6 for each additional port you wish to configure. 7.8: Click on the save button, the changes will take effect immediately.

Result

Password authentication will now be required when ever an iSCSI initiator connects to the system and the TCP port number will have to be changed to the value you have specified.

Related Topics

- 7.3 iSCSI Target Configuration
- Appendix E LED Indicators

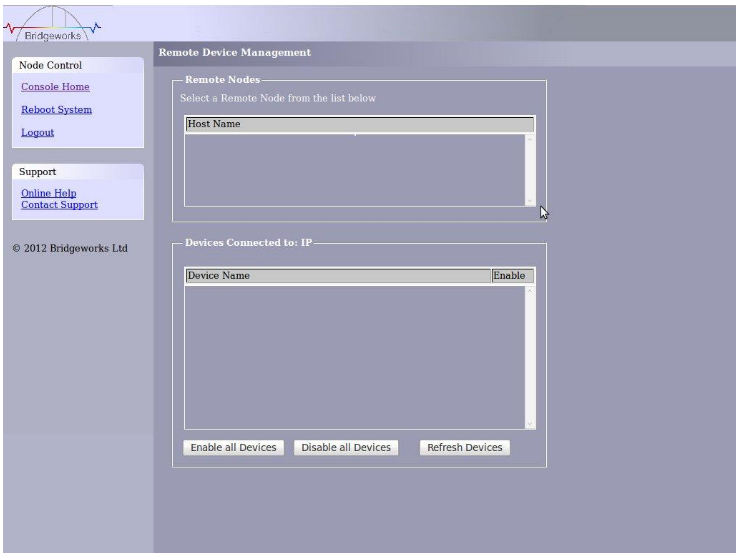
Step 8: Refreshing the Devices

Once you have configured the devices and ports it may be necessary to refresh the devices on each of your Nodes to reflect any changes made in the previous steps. This step may not be necessary but is advised to make sure your Nodes are up to date.

The following steps should be implemented for Example 1: **Node A** and Example 2: **Node C** and **D**.

Navigation

From the main menu select the “Remote Device Management” icon; the GUI will display the following screen.



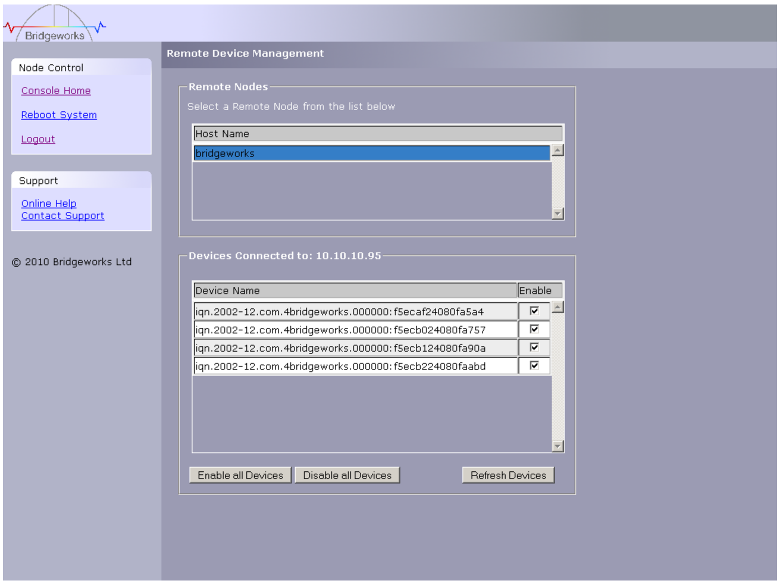
The Remote Device Management Page

Procedure: Refreshing the device list

Steps:	8.1: Select the Node you want to refresh the devices on from the “Host Name” list. When selected the Node will become blue. 8.2: Click on the “Refresh Devices” button at the bottom of the screen. The screen will go grey and a frame will appear with a blue loading bar. 8.3: Click on Ok to acknowledge the refreshed devices. 8.4: Repeat step 8.1 to 8.3 for each Node.

Result

Once completed a report will be returned informing you of the progress of the update. Every target device connected to the remote board that you have chosen to enable will be presented in the bottom list as shown below.



Select a Remote Node from the list below

Host Name
bridgeworks

Devices Connected to: 10.10.10.95

Device Name	Enable
iqn.2002-12.com.4bridgeworks.000000:f5ecaf24080fa5a4	☑
iqn.2002-12.com.4bridgeworks.000000:f5ecb024080fa757	☑
iqn.2002-12.com.4bridgeworks.000000:f5ecb124080fa90a	☑
iqn.2002-12.com.4bridgeworks.000000:f5ecb224080faabd	☑

The Remote Device Management Page with target devices attached to a remote Node

Related Topics

- 6.2 Remote Device Management

Step 9: iSCSI Sessions (Optional)

You will only need to complete this step if:

- You want to view any iSCSI sessions connected to this Node.
- You want to log out any iSCSI initiators connected to this Node.

If you don't require changing these settings skip to the next step.

The following Nodes Example 1: **Node B** and Example 2: **Node C**, **Node D** are the only Nodes that may require the following steps.

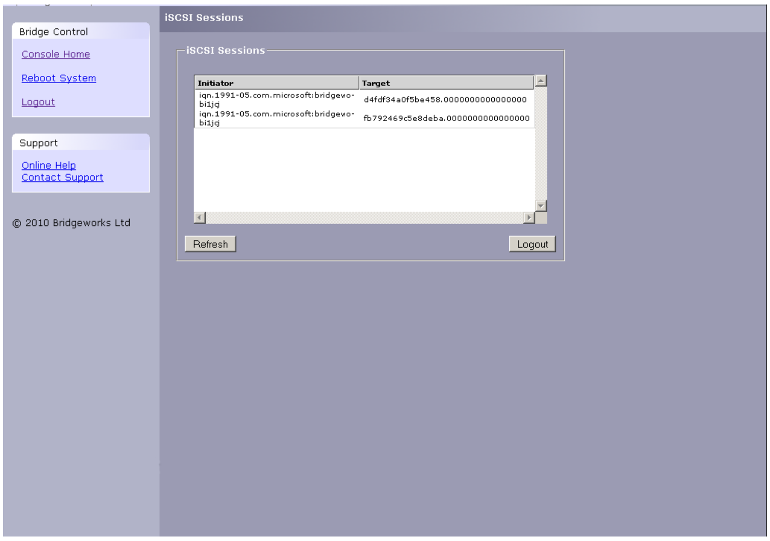
Information

Each initiator will open a session with each target device, these session are displayed in the iSCSI sessions table. It is possible for more than one host to be connected to any target device or one host to multiple target devices.

	Note: If you need help configuring your initiating machine see Appendix B for how to set up the Microsoft iSCSI initiator.

Navigation

From the main menu click the "Remote Device Management" link, the GUI will display the following screen.



Initiator	Target
iqn.1991-05.com.microsoft:bridgewo-bi1jg	d4fdf34a0f5be458.0000000000000000
iqn.1991-05.com.microsoft:bridgewo-bi1jg	fb792469c5e8deba.0000000000000000

iSCSI Sessions

Procedure: Logging out of an iSCSI session

Steps:	9.1: Select session from the list you want to logout from, when selected the background colour will become blue. 9.2: Click on the logout button, the initiator will be instantly logged out.

	Note: Many initiators are configured to automatically reconnect after completing the logout request. If this is the case then the connections window may not show any change.

Result

Any iSCSI sessions that have been logged out from will no longer be present in the table.

Related Topics

- 6.2 Remote Device Management

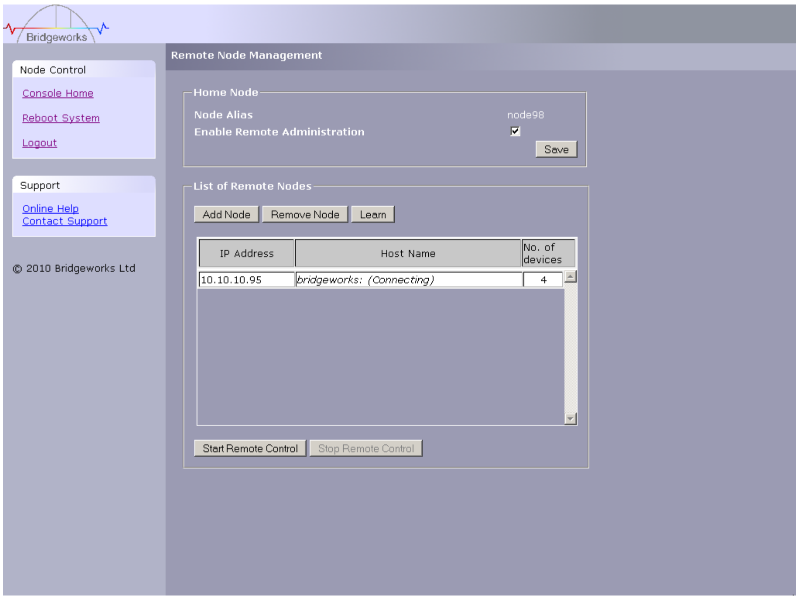
Step 10: Instigating the Learn Process

This procedure will “kick start” the Artificial Intelligence module to start learning the characteristics of the link network. Once it has completed it will store these values in memory ready for use when data transfer starts.

The following Nodes Example 1: **Node A** and Example 2: **Node C**, **Node D** are the only Nodes that may require the following steps.

Navigation

From the root menu select the remote Node Management icon; the GUI will display the following screen.



Node Alias node98

Enable Remote Administration ☑

IP Address	Host Name	No. of devices
10.10.10.95	*bridgeworks: (Connecting)*	4

Remote Node Management

Procedure: Initiate a learn

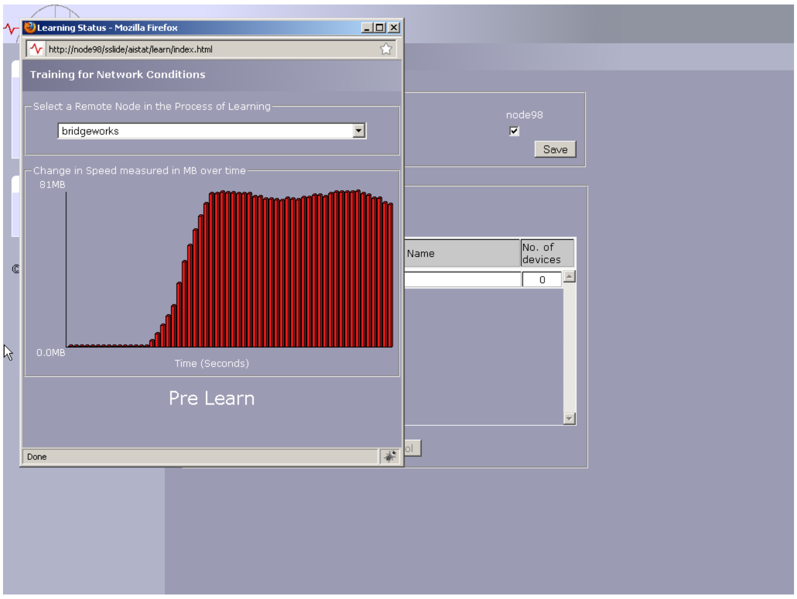
Steps:	10.1: Select the remote Node that you are going to use for the learn process from the List of Remote Nodes. 10.2: Click on the learn button just above the table.

	Note: The learn process can take up to 5 minutes to complete.

Steps:	10.3: Once this has completed, as indicated by the bottom text displaying “Learn Complete”, the pop-up window can be closed. 10.4: Repeat step 10 for each of the Nodes you have added.

Result

A pop up window will display the learn transfer graph and once complete will display the words learn complete at the bottom of the screen.



Learning Status - Mozilla Firefox

http://node98/sslide/aistat/learn/index.html

Training for Network Conditions

Select a Remote Node in the Process of Learning: bridgeworks

A Node in the process of a learn

Related Topics

- 6.1 Remote Device Management

4.4 Installation Complete

Congratulations. You have now completed the installation guide. If you need help configuring your initiating machine see Appendix B for how to set up the Microsoft iSCSI initiator. The next section covers each of the web interfaces functionality in more detail, if this still does not provide you with enough information please contact your reseller.

5.0 Network Configuration

This section will detail the operations of the following Network Configurations:

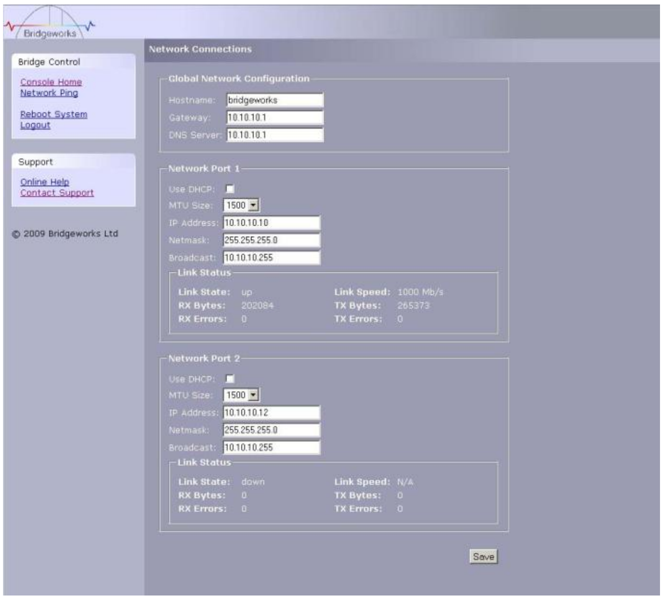
- 5.1 Connections
- 5.2 Passwords and Security
- 5.3 Network Services

5.1 Connections

This configuration page will allow the administrator to configure network interface settings and to view network statistics.

From within the main menu select the Network Control icon under the Network section

The GUI will now display the following window



Network Connections

Global Network Configuration
Hostname: bridgeworks
Gateway: 10.10.10.1
DNS Server: 10.10.10.1

Network Port 1
Use DHCP: □
MTU Size: 1500
IP Address: 10.10.10.10
Netmask: 255.255.255.0
Broadcast: 10.10.10.255
Link Status
Link State: up Link Speed: 1000 Mb/s
RX Bytes: 202084 TX Bytes: 265373
RX Errors: 0 TX Errors: 0

Network Port 2
Use DHCP: □
MTU Size: 1500
IP Address: 10.10.10.12
Netmask: 255.255.255.0
Broadcast: 10.10.10.255
Link Status
Link State: down Link Speed: N/A
RX Bytes: 0 TX Bytes: 0
RX Errors: 0 TX Errors: 0

Network Connections

The SANSlide Node has two GbE network ports. One is used for the management port and one is used for the link between the SANSlide Nodes. The left hand physical port is designated as port 1 in the above window and the right hand port as port 2

Setting the Hostname

In this box enter the name you wish to use to address this Node in the future. We suggest that you use a name that is relevant to its location and/or its purpose.

Note: If you select the DHCP mode, ensure your DHCP server is set to automatically update the DNS server.

Setting the MTU

Enabling larger frames on a jumbo frame capable network can improve the performance of your backup operations. Jumbo frames are Ethernet frames that contain more than 1500 bytes of payload (MTU). Before enabling jumbo frames, ensure that all the devices/hosts located on the network support the jumbo frame size that you intend to use to connect to the Node. If you experience network related problems while using jumbo frames, use a smaller jumbo frame size. Consult your networking equipment documentation for additional instructions.

Some networking switches require you to specify the size of the jumbo frame (MTU) when enabling, as opposed to a simple enable command. On these switches it might be required to add the necessary bytes needed for the frame header (i.e., header information + MTU). Typical header size is 28 bytes, so a 9000 byte MTU would translate to 9028 byte setting. Refer to your switch documentation to understand what the maximum frame size settings are for your switch.

Setting the IP Address

There are two possibilities when configuring the IP address of the iSCSI Node:

- DHCP - this means the Node will seek out the DHCP sever on your network and obtain an IP address from the server each time it powers up.

- Static IP - the IP address set in this page will be the IP address the unit will use each time it powers up.

Depending on the configuration, either click the DHCP button or set the Static IP address.

Note: If you select the DHCP mode, ensure your DHCP server is set to automatically update the DNS server.

Setting the Subnet Mask

If the Node is configured to use DHCP the net mask will be issued from the DHCP server. If you are using static IP address enter the IP mask in this box.

Committing the Changes

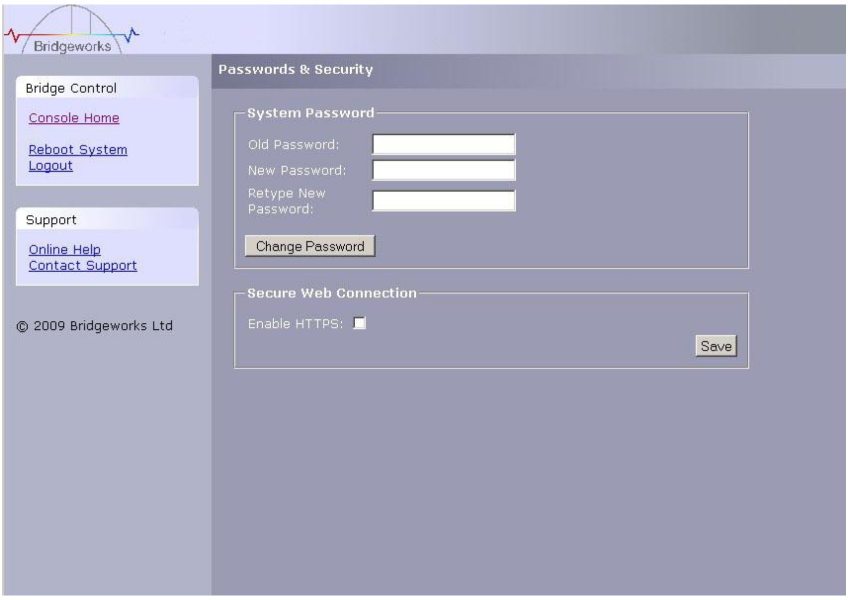
Click the save button to save these parameters and then click the reboot option in the left hand pane.

5.2 Passwords and Security

This configuration page will allow the administrator to change the access password for the GUI.

From within the main menu select the Password and Security icon under the Network section.

The GUI will now display the following window



Passwords and Security

To change your password, type the existing password and the new password into the appropriate boxes and press save.

Secure Connection – by clicking this box it will force all further transactions with the GUI to be done via a secure, encrypted HTTPS connection.

Once you have clicked this option, save the configuration and log out then log in again.

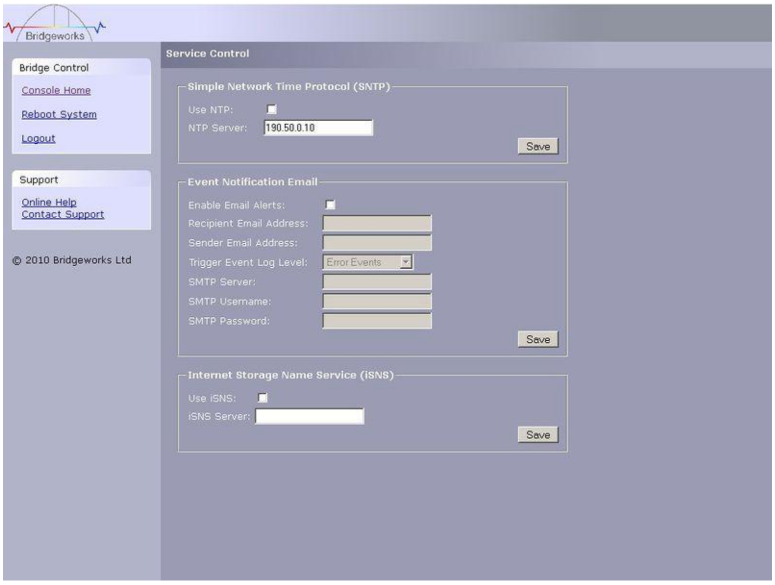
If you have lost your password please follow the steps in the Lost Password section of the Trouble Shooting chapter.

5.3 Network Services

This configuration page will allow the administrator to configure the IP addresses for the Network Time Domain.

From within the main menu select the Service Control icon under the Network section.

The GUI will now display the following window



Service Control

Simple Network Time Protocol (SNTP)

Use NTP: □
NTP Server: 190.50.0.10

Event Notification Email

Enable Email Alerts: □
Recipient Email Address:
Sender Email Address:
Trigger Event Log Level: Error Events
SMTP Server:
SMTP Username:
SMTP Password:

Internet Storage Name Service (iSNS)

Use iSNS: □
iSNS Server:

Service Control

5.3.1 NTP

The Network Time Protocol (NTP) is a protocol for synchronising the clocks of computer systems over the IP network. This feature is particularly useful when viewing the logs to determine the time an event occurs.

To enable NTP on the Node, click the tick box and enter the IP address for the NTP Server and then click the save button.

5.3.2 Email Alerts

The SANSlide Node can notify a systems administrator when certain level log events are observed in the Nodes logs.

To enable email alerts on the Node, click the tick box next to “Enable Alerts”, this will allow you to alter the contents of the currently greyed out fields. The following fields need to be completed.

Recipient Email Address – This is the email address to which the emails will be sent.

Senders Email Address - This is the email address that emails will be sent from. This can be any address and does not have to be genuine; which is useful for email filtering. For example entering in logs@4bridgeworks.com would allow emails from this address to be filtered to a specified folder in the users email client.

Trigger Event Log Level – This allows the user to specify what severity of event will trigger the log to be emailed with Critical Events being the most severe and Warning Events being the least. For each level picked the higher level logs will also be emailed, for example selecting Error Events will also send all Critical Events.

Below are examples of events that will be sent for each log level

- Critical: The Node is running at non recommended temperatures
- Error: The Node was Unable to connect to another Node
- Warning: A Remote Controlled GUI Session has been stopped

Note: For the following details consult your Network Administrator.

SMTP server – The IP address of the Mail Server that will handle the transport of the event emails.

SMTP Username – The username required to allow the use of the SMTP Server.

SMTP Password – The password required to allow the use of the SMTP Server.

5.3.3 iSNS

Internet Storage Name Service allows automated discovery, management and configuration of each iSCSI resource from a central point. If this option is enabled the Node will register its resources with a central iSNS server. To enable iSNS on the Node, click the tick box and enter the IP address for the iSNS Server and click the save button.

6.0 SANSlide Configuration

This section will detail the operations of the following SANSlide Configurations:

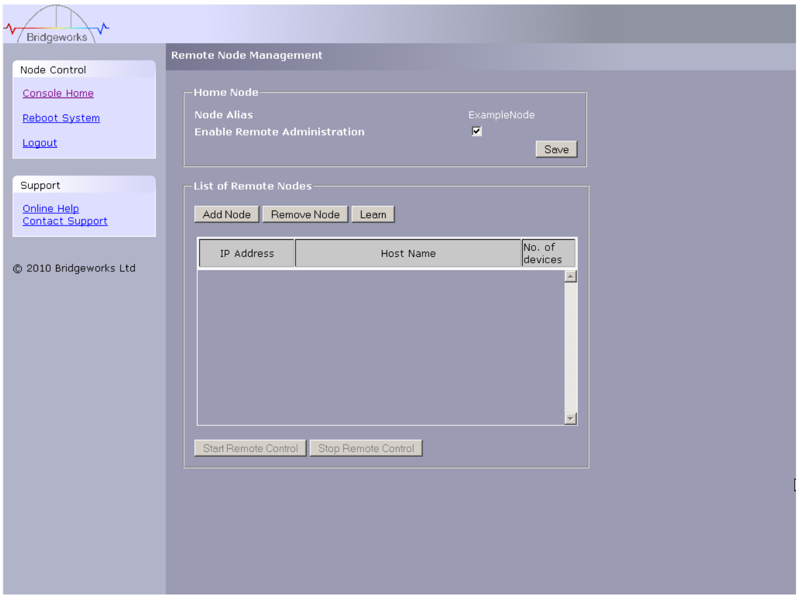
- 6.1 Remote Node Management
- 6.2 Remote Device Management
- 6.3 Transfer Statistics

6.1 Remote Node Management

This configuration page will allow the adding and removing of Nodes, the instigation of a learning cycle and the ability to take remote control of other Nodes.

From within the main menu select the Remote Node Management icon under the Network section.

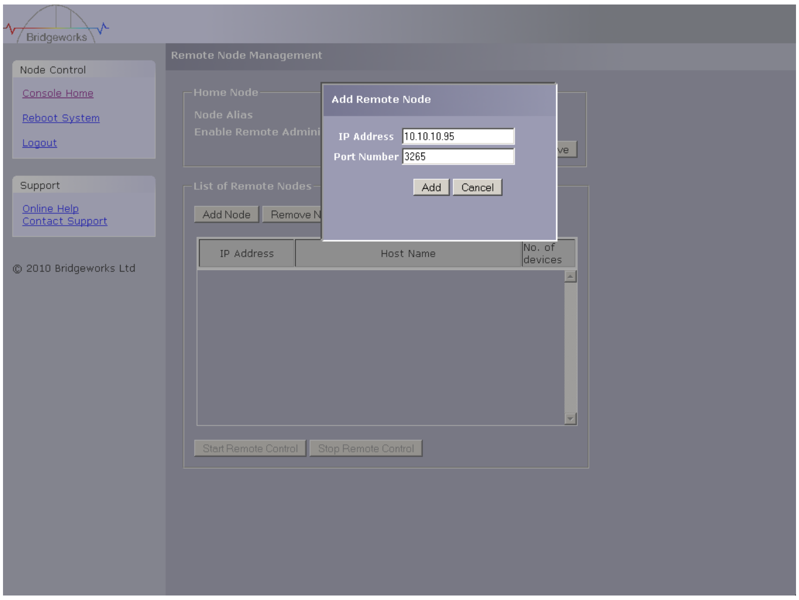
The GUI will now display the following window



Node Alias ExampleNode
Enable Remote Administration ☑

Remote Node Management

To add a Node, click on the “Add Node” button and then add the IP address of the Node to be connected to in the window as shown below, finally click the Add button.



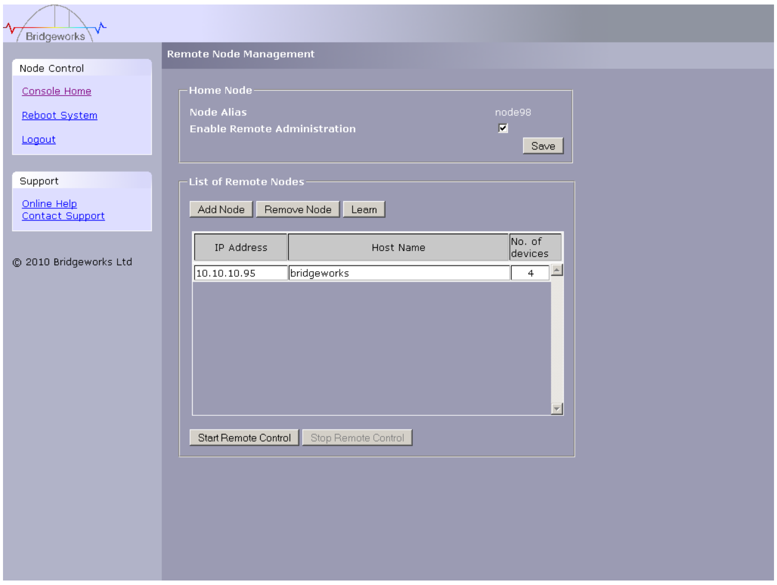
IP Address 10.10.10.95
Port Number 3265

Remote Node Management: adding a Node

The unit will then search for the Node on the Link Network, which will be displayed with a progress bar.

Once completed a window will appear with the Nodes name and the number of target devices attached to that Node. Any remote Node that has been added to the local Node in this way will be automatically saved, and will restore on reboot until the Node is removed.

The remote Node should then be displayed on the remote Node list as shown below.



Node Alias node98
Enable Remote Administration ☑

IP Address	Host Name	No. of devices
10.10.10.95	bridgeworks	4

Remote Node Management: with a Node added

To remove a Node that has been added simply select the Node from the list you want to remove and click the Remove Node button. A confirmation box will appear, click OK to continue.

6.1.1 Remote Control

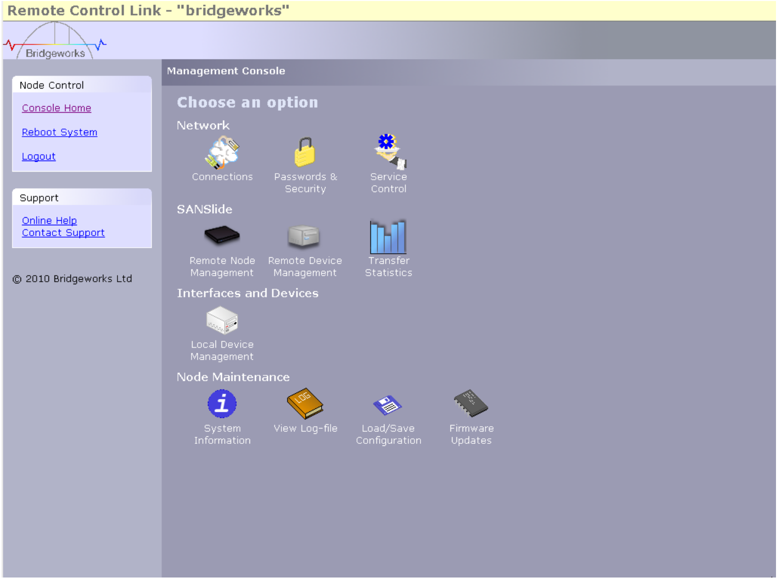
During the set up of your Nodes it may not be possible to directly access the web interface on a Node you want, “remote control” can be used to take control of any other Node added to your local Node.

To stop or allow other Nodes to take remote control of the Node you are currently using there is a checkbox within the home Node section at the top of the page. Select the checkbox if you want to allow other users to take control, deselect it if not. Once you have chosen click the save button.

Highlight the Node you wish to connect to by clicking the Node in the remote Node list and then the Start Remote Node Control button at the bottom of the list.

The web interface will now display the login screen of the remote Node as normal, and you login in the normal way using the credentials of the remote Node.

Whenever a remote control session is underway there will be a yellow bar at the top of the web interface which will contain the name of the Node you are connected to, as illustrated below.



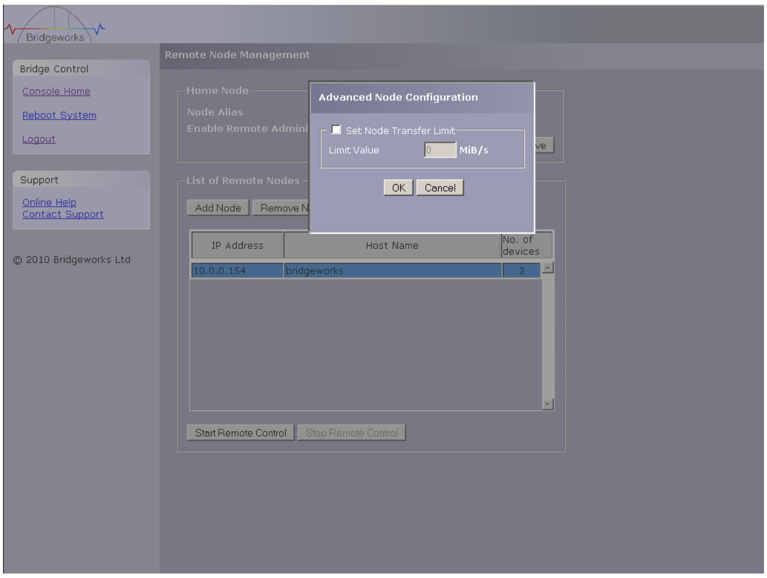
A remote Node under Remote Control

If you close down the window or tab containing the remote control session you can navigate back at any point to the Remote Node Management page on your Local Node, select the Node you had previous remote control over and click the “Reload Remote Window” button.

When you have finished configuring the remote Node, clicking “Stop Remote Control” from the Remote Node Management page will end the remote control session.

6.1.2 Configuring a Node

SANSlide will always attempt to get the best performance possible for the data it is transferring, however there may be other traffic on your network that will also need to accesses a share of your links bandwidth. The limit is induced on a per Node bases to limit the amount of bandwidth on a Node link click on the Node from the list and click on the “Configure Node” button an additional menu will appear as illustrated below.



Advanced Node Configuration

□ Set Node Transfer Limit

Limit Value 0 MiB/s

OK Cancel

IP Address	Host Name	No. of devices
10.0.0.154	bridgeworks	2

Configuring a Node

To set a limit click on the Set Node Transfer Limit checkbox, which should now allow the text box below to become editable. Type in a value you desire with a minimum possible value of one megabyte and click the OK button.

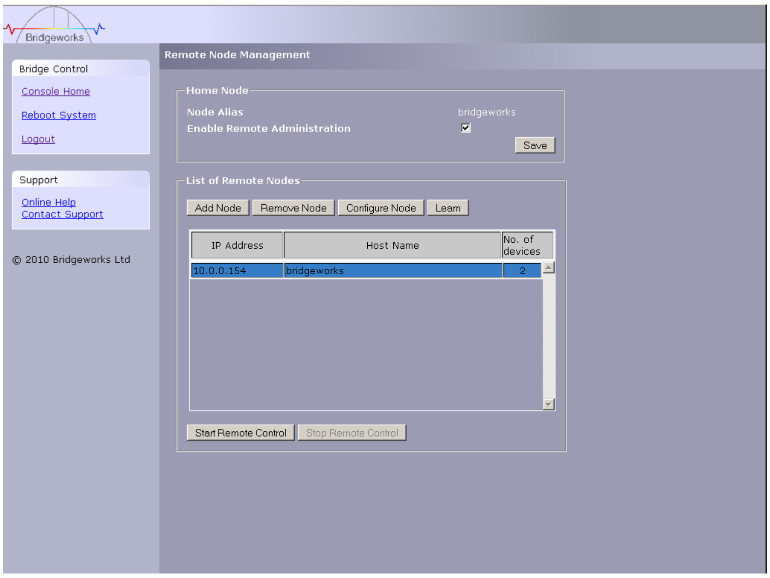
To remove a limit click on your chosen Node and click the configure Node button, uncheck the Set Node Transfer Limit checkbox and click "OK". The limit will now be lifted.

Note: Any changes to the bandwidth limit will become instantly effective.

6.1.3 Learning

This procedure will "kick start" the Artificial Intelligence module to start learning the characteristics of the link network. Once it has completed it will store these values in the memory flash ready for use when data transfers start.

From the root menu select the remote Node management icon; the GUI will display the following screen.



© 2010 Bridgeworks Ltd

Remote Node Management

Home Node

Node Alias bridgeworks

Enable Remote Administration ☑

List of Remote Nodes

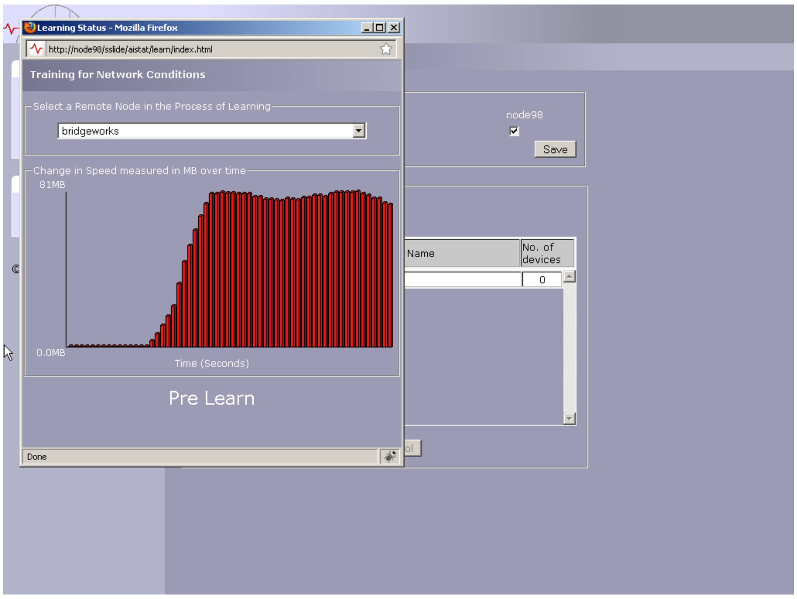
IP Address	Host Name	No. of devices
10.0.0.154	bridgeworks	2

Remote Node Management

Select the remote Node that you are going to use for the learn process from the List of Remote Nodes window and then click on the learn button just above the window. You can start Multiple Nodes learning in this way simultaneously by clicking on each one and clicking learn.

	Note: The learn process can take up to 5 minutes to complete.

The GUI will, in another window display the learn transfer graph as shown below.



Learning Status - Mozilla Firefox

http://node98/sslide/aistat/learn/index.html

Training for Network Conditions

Select a Remote Node in the Process of Learning: bridgeworks

Change in Speed measured in MB over time

Pre Learn

Done

node98 ☑

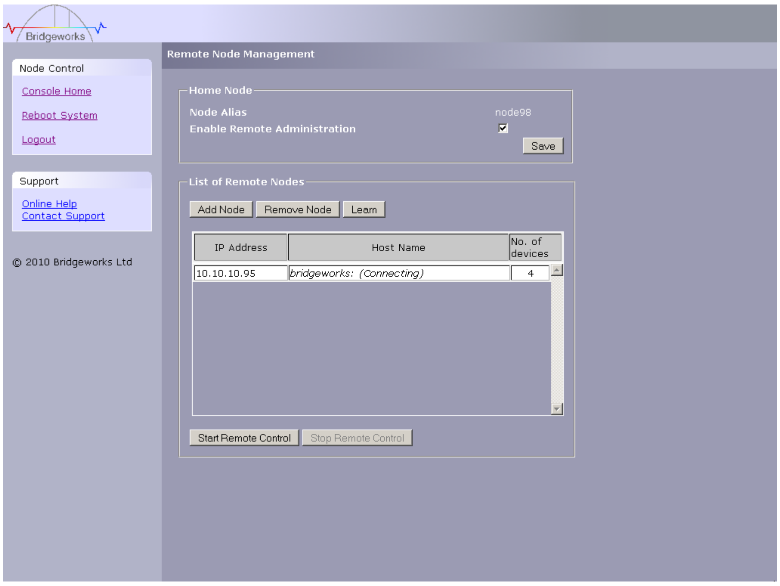
A Node in the process of a learn

Each Node in the process of a learn can be viewed by clicking on the drop down list of Nodes and selecting the one you wish to monitor.

Once this has completed, as indicated by the bottom text displaying “Learn Complete”, the Pop-up window can be closed.

6.1.4 Restoring of a Node

When a Node has been restarted and it is in the process of re-establishing its link to another Node, the words Connecting may appear next to the Nodes name in brackets and the text will be in italics as shown below.



Remote Node Management

Home Node

Node Alias node98

Enable Remote Administration ☑

List of Remote Nodes

IP Address	Host Name	No. of devices
10.10.10.95	*bridgeworks: (Connecting)*	4

A Node in the process of restoring its Links

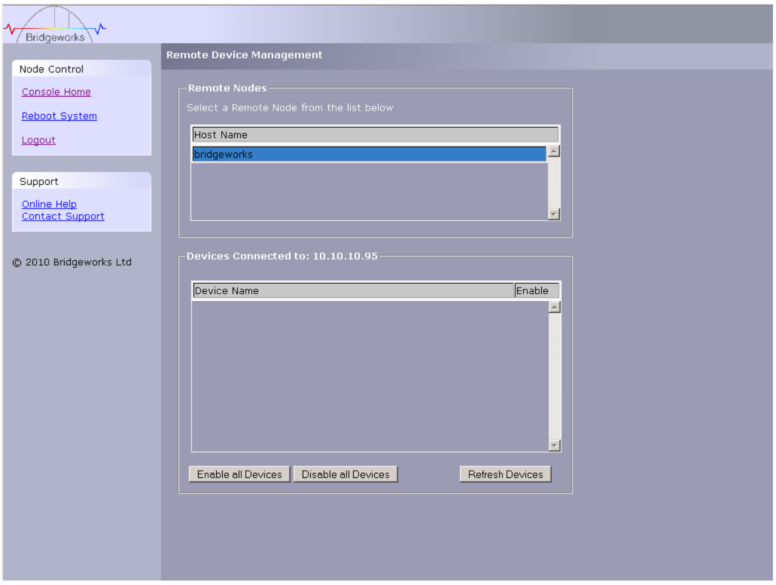
During this time it is not possible to use the features of a Node apart from remove until the connection has been established. A repeat attempt at connecting to a Node can take up to a minute and if the Node fails it will continually retry. Any newly discovered Target Devices would be added automatically.

6.2 Remote Device Management

This configuration page will allow the Adding and Removing of Nodes, the instigation of a learning cycle and the ability to take remote control of other Nodes.

From within the main menu select the Remote Node Management icon under the Network section.

The GUI will now display the following window



Select a Remote Node from the list below

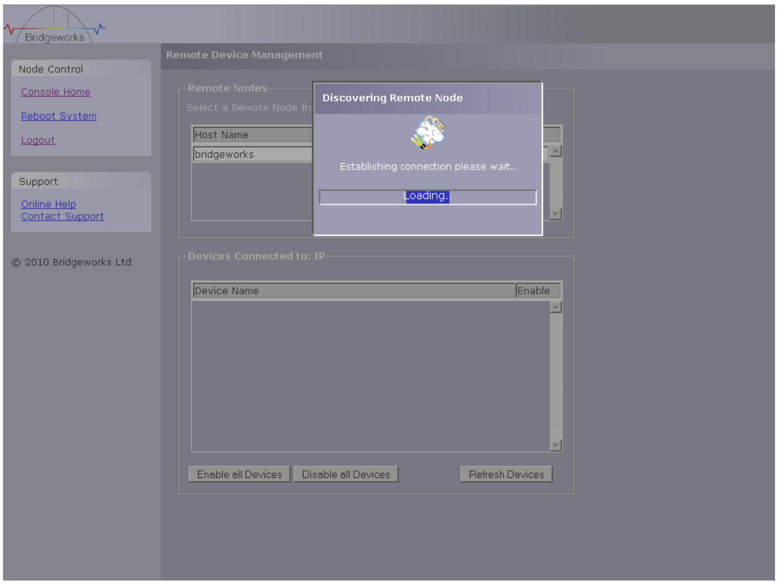
bridgeworks

Devices Connected to: 10.10.10.95

Remote Device Management

To refresh the devices on this list, select the Node you want to refresh the devices on from the “Host Name” list and click on it. When successfully selected the Node will become blue.

Click on the “Refresh Devices” button at the bottom of the screen. The screen will go grey and a frame will appear with a blue loading bar as shown below.



Select a Remote Node fr

bridgeworks

Discovering Remote Node

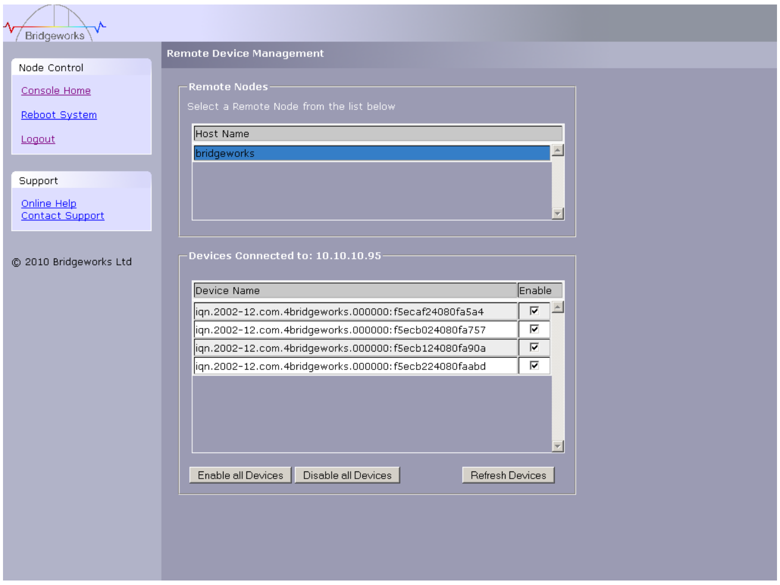
Establishing connection please wait..

Loading.

Devices Connected to: IP

The Remote Device Management page in the process of an update

When the loading bar is complete a report will be returned informing you of the progress of the update.



Remote Nodes

Select a Remote Node from the list below

Host Name
bridgeworks

Devices Connected to: 10.10.10.95

Device Name	Enable
iqn.2002-12.com.4bridgeworks.000000:f5ecaf24080fa5a4	☑
iqn.2002-12.com.4bridgeworks.000000:f5ecb024080fa757	☑
iqn.2002-12.com.4bridgeworks.000000:f5ecb124080fa90a	☑
iqn.2002-12.com.4bridgeworks.000000:f5ecb224080faabd	☑

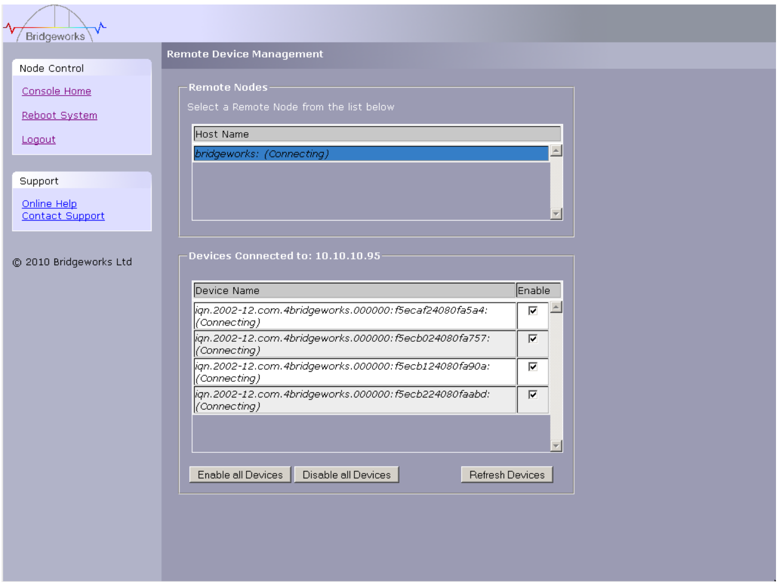
The Remote Device Management Page, which has a Node with multiple Target Devices

6.2.1 Enabling / Disabling a Target Device

Disabling a target device will prevent it from being presented to your initiating device. All target devices are enabled by default. To disable a single device, uncheck the tick box next to the targets name. To enable a device, click the checkbox and make sure it has a visible tick within it.

6.2.2 Restoring of Devices

When a Node has been restarted and it is in the process of re-establishing its link to another Node the word Connecting may appear next to the Nodes name, the target devices name in brackets and the text will be in italics as shown below.



Remote Nodes

Select a Remote Node from the list below

Host Name
bridgeworks: (Connecting)

Devices Connected to: 10.10.10.95

Device Name	Enable
iqn.2002-12.com.4bridgeworks.000000:f5ecaf24080fa5a4: (Connecting)	☑
iqn.2002-12.com.4bridgeworks.000000:f5ecb024080fa757: (Connecting)	☑
iqn.2002-12.com.4bridgeworks.000000:f5ecb124080fa90a: (Connecting)	☑
iqn.2002-12.com.4bridgeworks.000000:f5ecb224080faabd: (Connecting)	☑

The Remote Device Management page in the process Linking Together Nodes

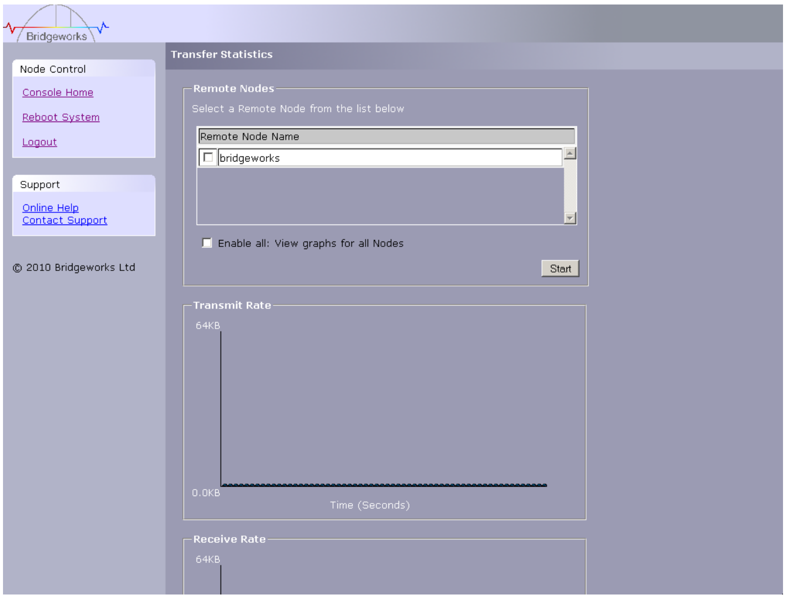
All the functionality that can be used when a Node is active can be used whilst a Node is connecting but the effects will not occur until the link is up.

6.3 Transfer Statistics

This configuration page will allow you to monitor in real time the performance of a link over the span of a minute.

From within the main menu select the Remote Node Management icon under the Network section.

The GUI will now display the following window



© 2010 Bridgeworks Ltd

Select a Remote Node from the list below

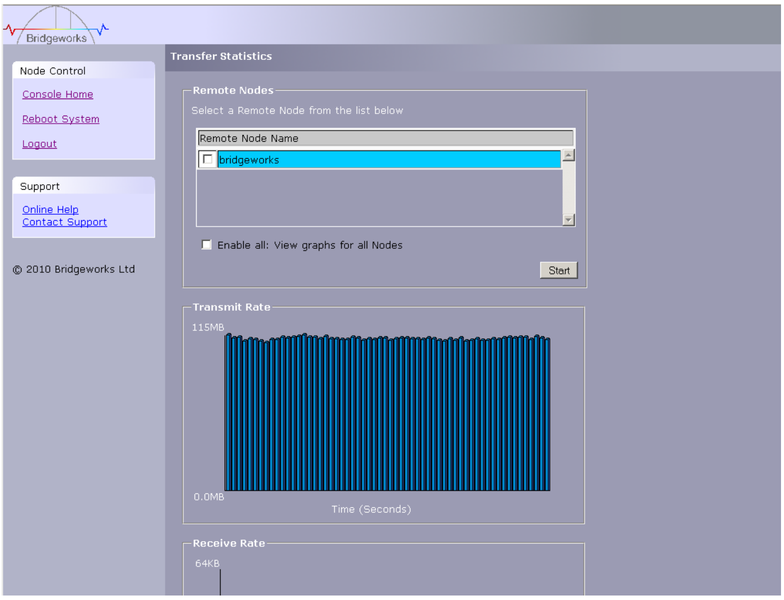
Remote Node Name
□ bridgeworks

□ Enable all: View graphs for all Nodes

The Transfer Statistics Page without a Node being selected.

This page will show you both the transmit and the receive rate for any selected Nodes, the transmit rate for a Node is in blue and the receive rate is in red. To view a Nodes transfer rate click on the name of the Node from the list and graphing will start automatically.

Note: Because these parameters are always in a state of continual monitoring by the AI clicking to view these figures will not affect the performance of the data transfer.



Transfer Statistics

Remote Nodes

Select a Remote Node from the list below

Remote Node Name
□ bridgeworks

□ Enable all: View graphs for all Nodes

Transmit Rate

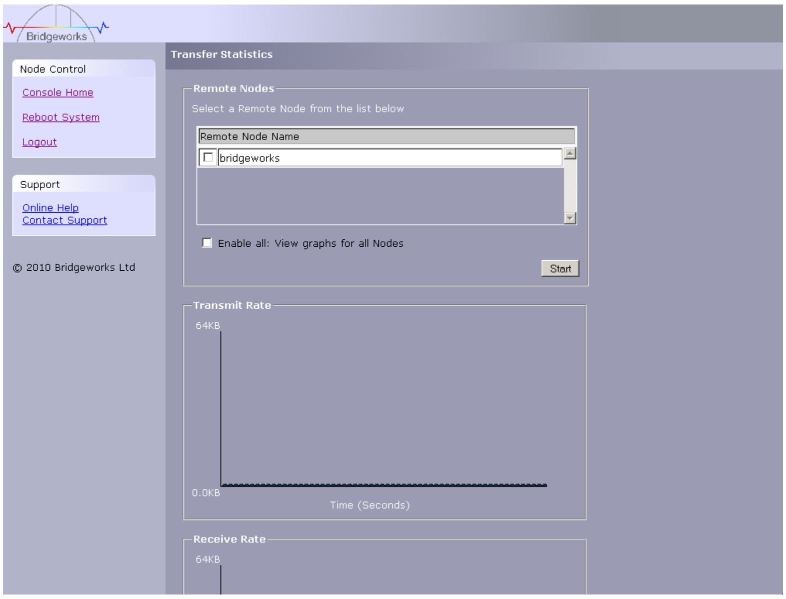
Receive Rate

The Transfer Statistics Page with a Selected Node

To find out the IP address of a Remote Node leave the mouse over it and it will be displayed in a pop up box.

Offline

A Node will be offline if the link between two SANSlide Nodes has not been re-established after a system restart. You cannot start the monitoring of the Node until the link has been re-established.



Transfer Statistics

Remote Nodes

Select a Remote Node from the list below

Remote Node Name
□ bridgeworks

□ Enable all: View graphs for all Nodes

Transmit Rate

Receive Rate

The Transfer Statistics Page with the Node Offline

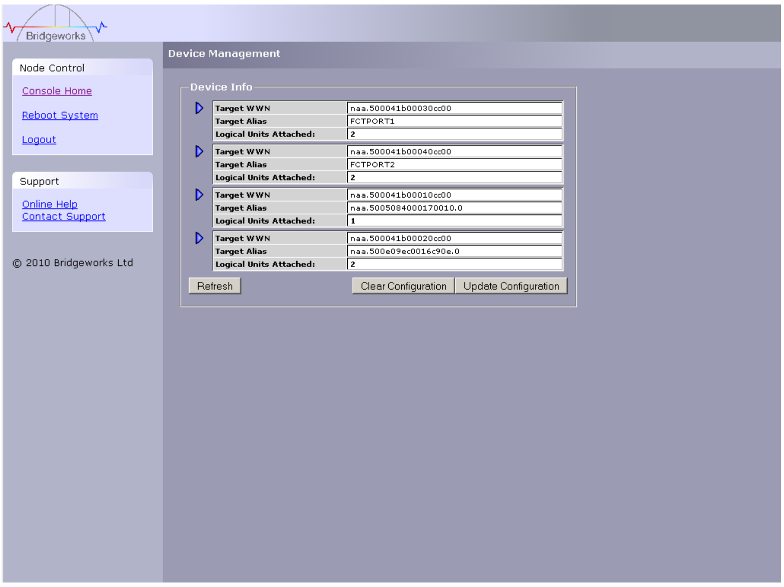
7.0 Interfaces and Devices Configuration

7.1 Local Device Management

This configuration page will allow you to view the different target devices that are connected to your Node.

From within the main menu select the Local Device Management icon under the Network section.

The GUI will now display the following window



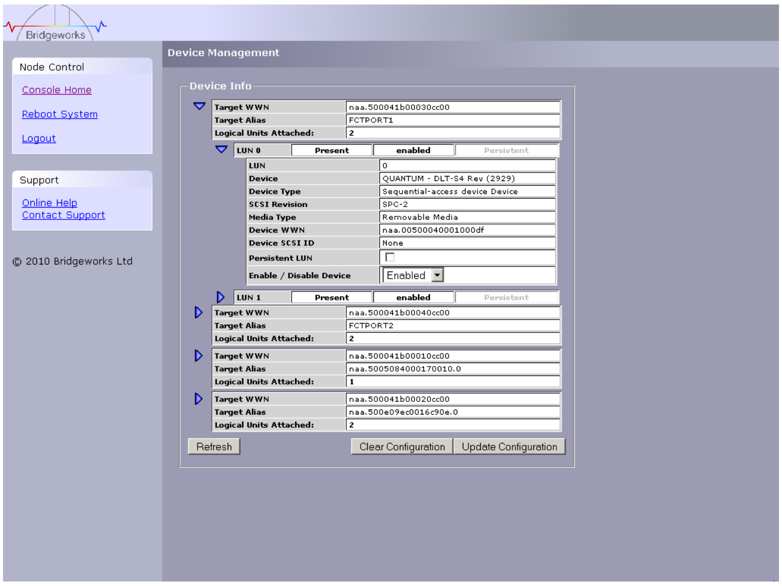
Device Management

Device Info

Target WWN	naa.500041b00030cc00
Target Alias	FCTPORT1
Logical Units Attached:	2
Target WWN	naa.500041b00040cc00
Target Alias	FCTPORT2
Logical Units Attached:	2
Target WWN	naa.500041b00010cc00
Target Alias	naa.5005084000170010.0
Logical Units Attached:	1
Target WWN	naa.500041b00020cc00
Target Alias	naa.500e09ec0016c90e.0
Logical Units Attached:	2

Local Device Management Page

Next to each target device is a blue triangle. Clicking this triangle will expand out this device and give you full details such as the device's name and type as shown in the image below.



Device Management

Device Info

Target WWN	naa.500041b00030cc00
Target Alias	FCTPORT1
Logical Units Attached:	2

LUN 0	Present	enabled	Persistent

LUN	0
Device	QUANTUM - DLT-S4 Rev (2929)
Device Type	Sequential-access device Device
SCSI Revision	SPC-2
Media Type	Removable Media
Device WWN	naa.00500040001000df
Device SCSI ID	None
Persistent LUN	□
Enable / Disable Device	Enabled

LUN 1	Present	enabled	Persistent

Target WWN	naa.500041b00040cc00
Target Alias	FCTPORT2
Logical Units Attached:	2
Target WWN	naa.500041b00010cc00
Target Alias	naa.5005084000170010.0
Logical Units Attached:	1
Target WWN	naa.500041b00020cc00
Target Alias	naa.500e09ec0016c90e.0
Logical Units Attached:	2

Local Device Management Page with the target device details expanded

7.1.1 Enabling / Disabling a Target Device

For each target device there are two possible actions, whether the device is enabled or not and if the device requires a Persistent LUN.

Each device is enabled by default. Disabling a device will prevent it from being available to another SANSlide Node or presented to an initiating device.

7.1.2 Saving

After any changes have been made click the Update Configuration button to make the changes permanent. If at any point you want to remove those changes click the Clear Configuration button.

7.2 Configuring and Connecting iSCSI Devices

7.2.1 Definitions

In order to understand the process of identifying and configuring devices on the SCSI bus for the server to communicate with it is necessary to understand some of the terms used by the menus

iSCSI Target Device

An iSCSI target device is device such as a disk drive, tape drive or RAID controller that is attached to the network. Each device is identified by an IQN.

iSCSI Qualified Name (IQN)

Anything connected to a network, be it a computer, printer or iSCSI device must have a unique identifier, such as an IP address, to enable other devices to communicate with it. With iSCSI devices (both targets and initiators) an extra level of identification in addition to the IP address is employed. This is called the IQN. The IQN includes the iSCSI Target's name and an identifier for the shared iSCSI device.

Example: 2002-12.com.4bridgeworks.sdt600a014d10: 5

7.2.2 Configuring Devices

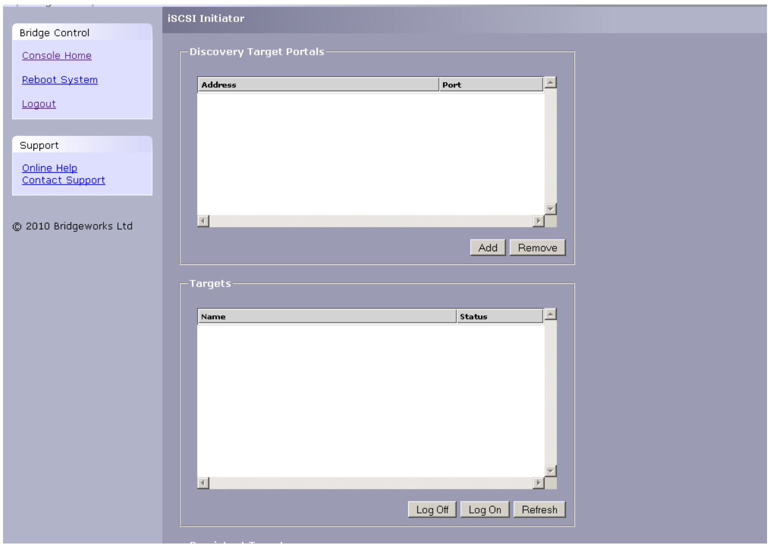
To add a device to the iSCSI Node requires 3 basic steps:

- Identify the iSCSI device(s) you wish to use
- Identify and logon to the iSCSI device(s)
- Identify and enable the iSCSI device(s) on the SCSI bus

The following sequence is repeated for each device you wish to connect to the iSCSI Node.

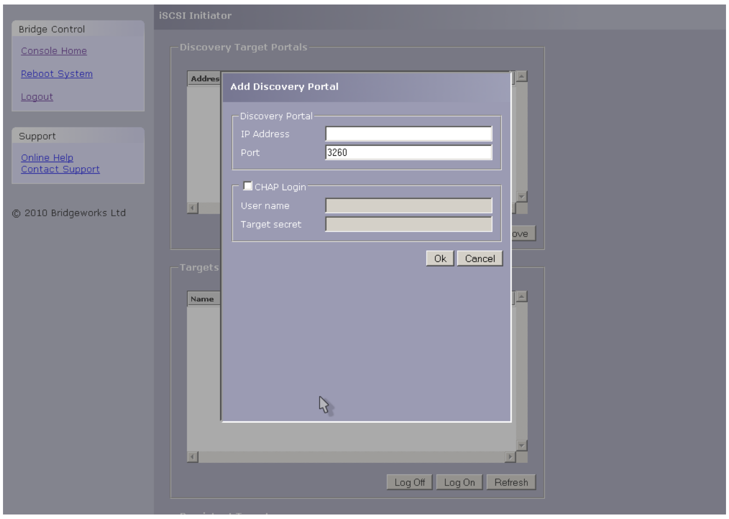
7.2.3 Adding an iSCSI discovery

From the main menu, click on the iSCSI Initiator logo.



iSCSI initiator page.

Click on the 'Add' in the 'Discovery Target Portals' window.



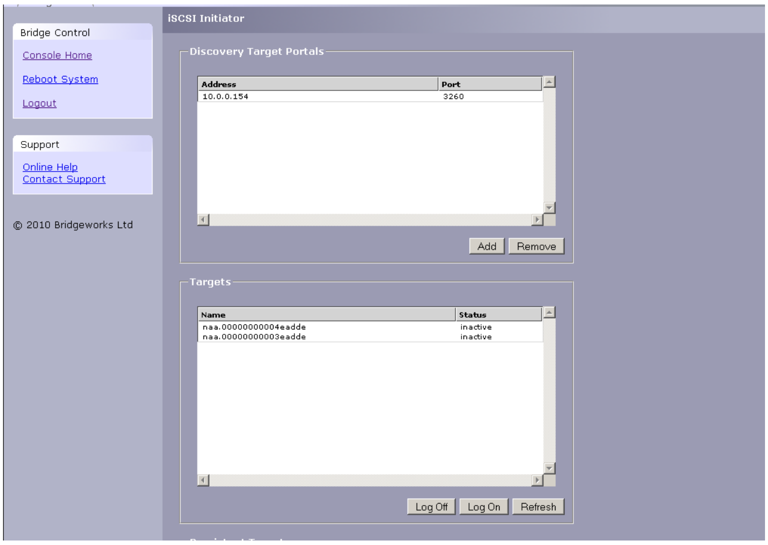
Port: 3260

Adding the IP address of the iSCSI target.

In the "Add Discovery Portal" window insert the IP address of the iSCSI target device you wish to connect to and source interface.

If the iSCSI device has CHAP enabled for discoveries then you will need to check the 'CHAP Login' box and fill in the username and password. When complete click on the 'ok' button

The unit will now go through a process called iSCSI Discovery. This will access the iSCSI Target Device and request the unit to report on the devices within it. Any devices found will appear in the Targets window below along with its IQN. If the iSCSI Target Device had more than one device attached, then all of these devices would be shown.



Address	Port
10.0.0.154	3260

Name	Status
naa.00000000004eadde	inactive
naa.00000000003eadde	inactive

iSCSI targets display list.

In the example above we can see that IP Address 10.0.0.154 has a two devices attached to it. The status of them is inactive; this is because at this point we have only made a Discovery request to the iSCSI Target Device. To enable the device an iSCSI logon function has to be performed.

7.2.4 Removing an iSCSI discovery

From the Discovery portals list select the IP address you wish to remove, when selected the background colour will change to blue. Click the remove button below, a message will appear saying

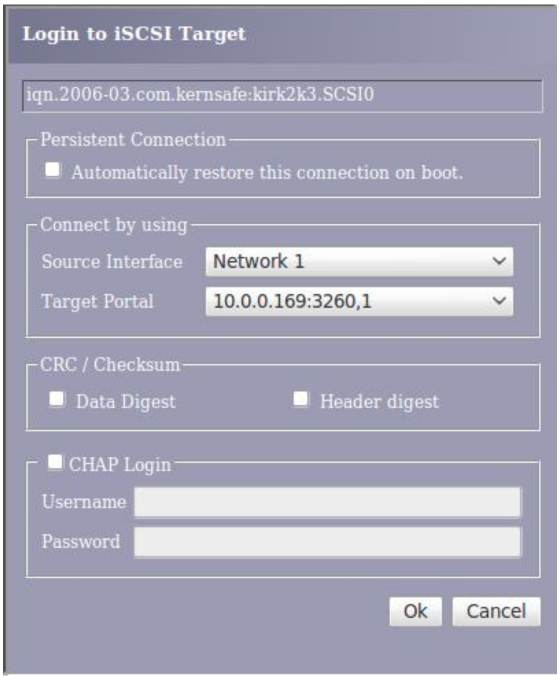
`“Are you sure you want remove the selected Discovery Portal?”`

Click the OK button if you wish the discovery to be removed.

7.2.5 Log On

To logon to an IQN, highlight the IQN by clicking on its entry in the Targets window and then click the ‘Log On’ button.

At this point a new window will appear.



Login to iSCSI Target

iqn.2006-03.com.kernsafe:kirk2k3.SCSI0

Persistent Connection

□ Automatically restore this connection on boot.

Connect by using

Source Interface: Network 1

Target Portal: 10.0.0.169:3260,1

CRC / Checksum

□ Data Digest □ Header digest

□ CHAP Login

Username

Password

Pop-up window for iSCSI Target Logon

7.2.6 Persistent Connection

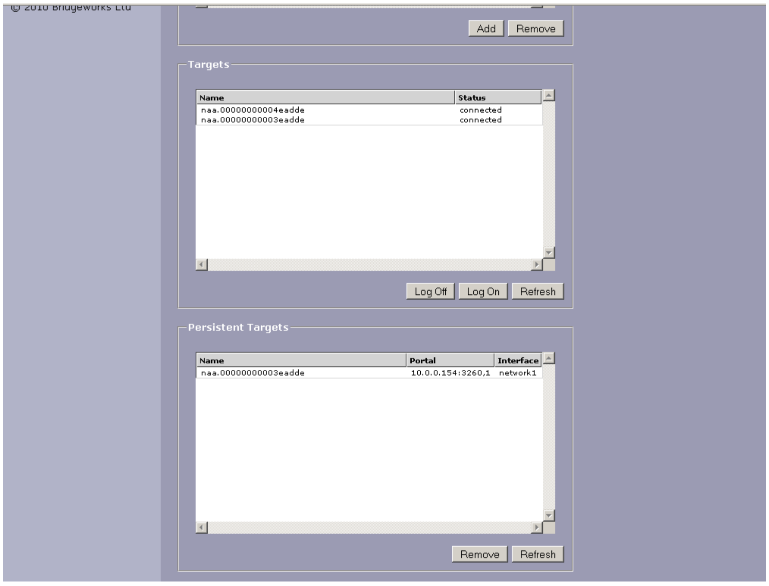
If you wish for the unit to connect to this IQN after a reset or reboot, then this box needs to be checked. It is recommended that this feature be enabled.

7.2.7 CHAP Login

If the iSCSI Target Device has CHAP enabled, check the tick box and enter the username and password to communicate with this device.

Once you have completed this window, click the OK button.

The Node should now display the IQN with the word “Connected” next to it. Repeat this process for all the required iSCSI Target Devices



© 2010 Bridgeworks Ltd

Targets

Name	Status
naa.00000000004eadde	connected
naa.00000000003eadde	connected

Persistent Targets

Name	Portal	Interface
naa.00000000003eadde	10.0.0.154:3260,1	network1

iSCSI with connected targets.

Note: If you enabled Persistent Connection these devices will be also displayed in the Persistent Targets window below the Targets window.

7.2.8 Log Off

From the Targets list select the target you wish to remove, when selected the background colour will change to blue. Click the log off button below, a message will appear saying

```
“Are you sure you want to Log Off?”
```

Click the OK button if you wish the target to become inactive.

7.2.9 Refresh Targets

If at a point after the initial discovery, your discovery device has had additional targets added to it, the refresh button will update the targets list to present those devices.

7.2.10 Remove

If a target has been made to be persistent it will appear in the persistent target list. To stop the target from restoring on reboot select the target from the persistent list, the background colour will become blue. Click on the remove button, a message will appear saying

```
“Are you sure you want to remove the selected persistent Target?”
```

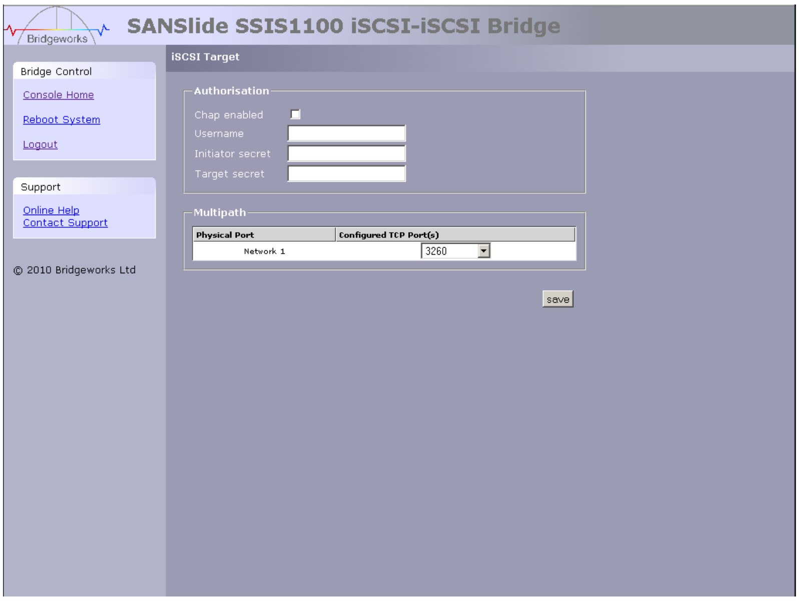
Click the OK button if you to remove the selected persistent target, cancel if not.

7.3 iSCSI Target Configuration

This configuration page will allow the administrator to configure the password and username for the CHAP authorisation on the Node.

CHAP is an authentication scheme used by servers to validate the identity of clients and vice versa. When CHAP is enabled, the initiator must send the correct username and target password to gain access to the iSCSI Node. The initiator secret is provided to allow iSCSI mutual CHAP. If mutual CHAP is selected on the initiator, the iSCSI Node will authenticate itself with the initiator using the initiator secret

From within the main menu select the iSCSI Target icon from the SCSI System group
The GUI will now display the following window



iSCSI Target

Authorisation

Chap enabled ☐
Username
Initiator secret
Target secret

Multipath

Physical Port	Configured TCP Port(s)
Network 1	3260

iSCSI Target Page

7.3.1 CHAP

To enable CHAP click the tick box and enter the following details

- Username – this is the same name as specified in the iSCSI host
- Initiator Secret – this is the password defined in the iSCSI host
- Target Secret - this is the password that the Node will send to the iSCSI Host.

7.3.2 Multi-path Settings

Multi-path is a method of sending data to an iSCSI target over multiple network connections. These network connections can be on the same physical network cable or separate network cables. By using multi-path, it is possible to increase the network bandwidth to send data over. A user may have a single iSCSI Session for an iSCSI target, but within that session may have multiple connections.

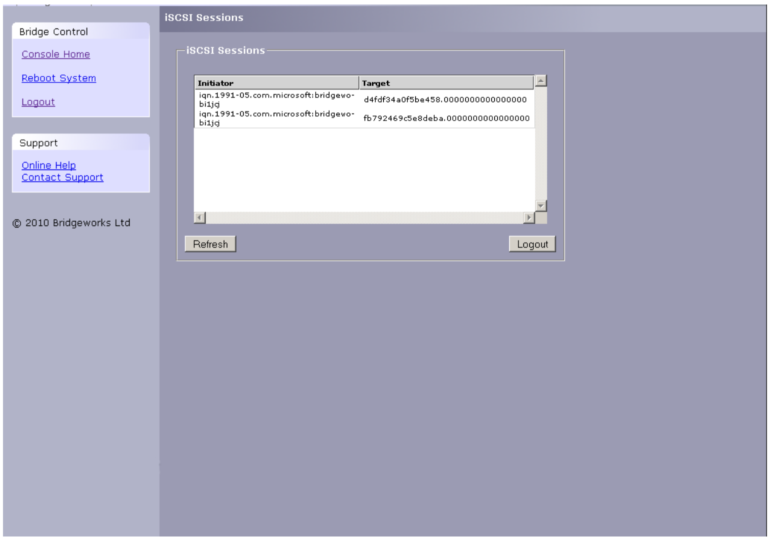
iSCSI uses two main network ports, 3260 and 860. Within the multi-path configuration the user can specify which ports will be made available to the initiator, 860, 3260 or both.

Note: See Appendix B for how to set up multi-path on the a Microsoft based Server

7.4 iSCSI Sessions

Each initiator will open a session with each target device; to review these connections select the iSCSI session's page from the SCSI group.

From within the main menu select the iSCSI Sessions icon from the SCSI System group
The GUI will now display the following window



Initiator	Target
iqn.1991-05.com.microsoft:bridgewo-bi1jg	d4fdf34a0f5be458.0000000000000000
iqn.1991-05.com.microsoft:bridgewo-bi1jg	fb792469c5e8deba.0000000000000000

iSCSI Sessions Page

This page lists the current connections i.e. logged on, from iSCSI hosts. It displays which initiator is connected to which target device.

Note: It is possible that more than one host to be connected to any target device or one host to multiple target devices.

Should it be required, it is possible to send a logout request to a host by highlighting the host connection and pressing the logout button.

Note: Many initiators are configured to automatically reconnect after completing the logout request. If this is the case then the connections window may not show any change.

8.0 Node Maintenance

The following section describes the various pages that are available to the administrator to monitor the performance and maintain the Node. The following operations will be detailed.

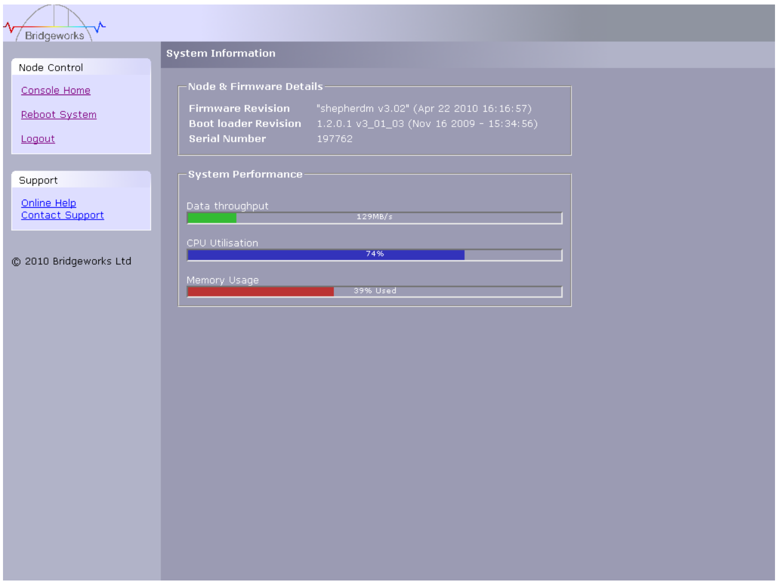
- 8.1 System Information
- 8.2 System Log
- 8.3 Firmware Updates
- 8.4 Saving the Configuration to disk
- 8.5 Restore Factory Defaults

8.1 System Information

This system information page will allow the administrator to view the performance of the Node

From within the main menu select the System Information icon from the Node maintenance section.

The GUI will now display the following window



System Information

Node & Firmware Details

Firmware Revision "shepherdm v3.02" (Apr 22 2010 16:16:57)
Boot loader Revision 1.2.0.1 v3_01_03 (Nov 16 2009 - 15:34:56)
Serial Number 197762

System Performance

Data throughput 129MB/s

CPU Utilisation 74%

Memory Usage 39% Used

System Information Page

Within the top window the following information is displayed:

- Current Firmware Level
- Bootloader revision
- Serial Number of the PCB within the Node

Within the lower window are 3 bar graphs, which provide an approximation of the following performance parameters.

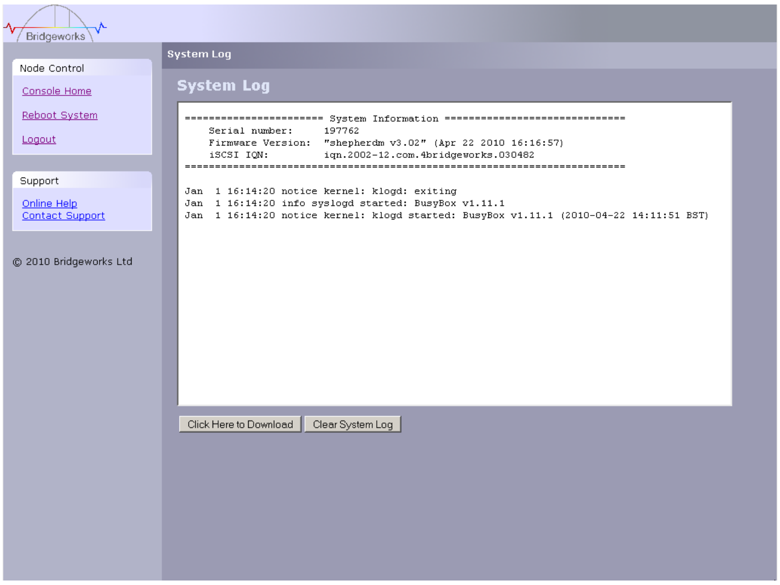
- Network Speed - This indicates the current performance in MB/s across the network.
- CPU - This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces
- Memory usage- This indicates the percentage of memory used by all processes

8.2 System Log

This system information page will allow the administrator to view the log status that the Node encounters whilst running.

From within the main menu select the View Log-file icon from the Node Maintenance section.

The GUI will now display the following window



```
====================== System Information ================================
    Serial number:     197762
    Firmware Version:  "shepherdm v3.02" (Apr 22 2010 16:16:57)
    iSCSI IQN:         iqn.2002-12.com.4bridgeworks.030482
==========================================================================

Jan  1 16:14:20 notice kernel: klogd: exiting
Jan  1 16:14:20 info syslogd started: BusyBox v1.11.1
Jan  1 16:14:20 notice kernel: klogd started: BusyBox v1.11.1 (2010-04-22 14:11:51 BST)
```

The System Log Page with the Log cleared

Below the log display pane are two options:

- Clear system logs – this will delete the current and saved logs within the Node
- Download – this will download the log files to your local disk. You may be asked by our support team to email this log file to them to aid them in any problem resolution.

8.3 Firmware Updates

From time to time it may be necessary to upgrade the firmware within the Node. New versions contain resolutions to known issues as well as new features and improvements to the functionality of the Node. It is advisable to check on the latest release on a regular basis.
Where possible firmware on two communicating SANSlide Nodes should be kept consistent.

New versions of the firmware can be downloaded from the Bridgeworks web site at:

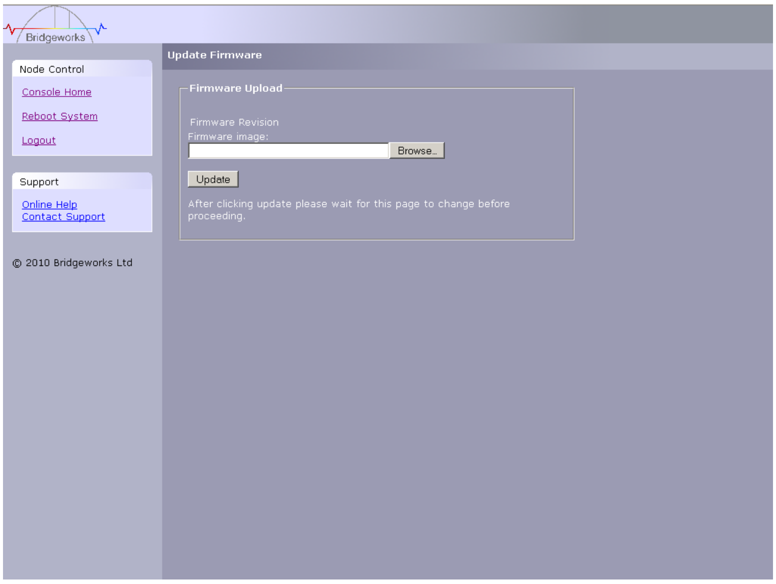
www.4bridgeworks.com/support/software.shtml

⚠	**Warning:** Ensure you have the correct firmware for your product – IF IN DOUBT ASK.

The Firmware Updates page will allow the administrator to load new firmware into the Node.

From within the main menu select the Firmware Updates icon from the Node Maintenance section.

The GUI will now display the following window



After clicking update please wait for this page to change before proceeding.

The Firmware Update Page

Once you have downloaded the new firmware to a local disk drive:

- Click on the browse button to locate the file you have downloaded from the website
- Then click on the update button.

Updating the firmware will take a few minutes after which it will be necessary to reboot the system to bring the new code into memory.

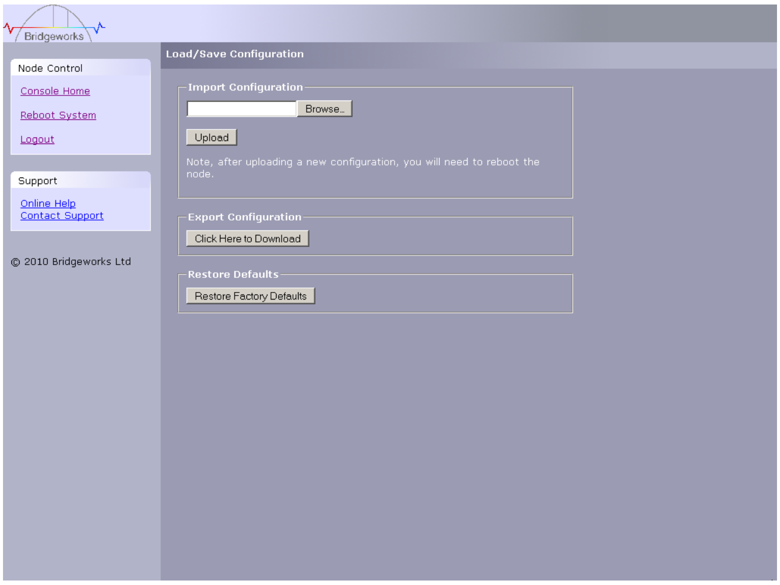
8.4 Saving the Configuration to Disk

Once you have finished configuring your Node we recommend that you save your configuration data to a local disk. By doing so you could save valuable time if the unit requires replacement or if a configuration is lost during upgrades.

It is also possible to create a “Boiler Plate” configuration and load this into each new Node as it is initialised. This can ease the rollout of multiple Nodes within an enterprise.

From within the main menu select the Load Save Configuration icon from the Node Maintenance section.

The GUI will now display the following window



Note, after uploading a new configuration, you will need to reboot the node.

The Load/Save Configuration Page

To save the configuration data click on the “Click here to Download” link from within the Export Configuration window located in the centre of the page.

Depending upon the browser you are using, select the option to “save file to disk”.

The Node will now download an encoded file that contains all the configuration settings for the Node.

To reload the configuration, click on the “Browse” button and locate the required configuration to upload into the Node. Once located click the upload button and the new configuration data will be uploaded.

Once completed, use the various configuration pages to make any further adjustments required and then reboot the system.

8.5 Restore to Factory Defaults

By clicking on this button all the parameters will be set back to the factory defaults. This includes IP address, hostname and passwords. We recommend that if you return the Node for maintenance that you reset to defaults to protect passwords and other sensitive information. If you are accessing your Node remotely over a SANSlide link, do not use this option as you wont be able to re-establish connection with your Node,

9.0 Trouble Shooting

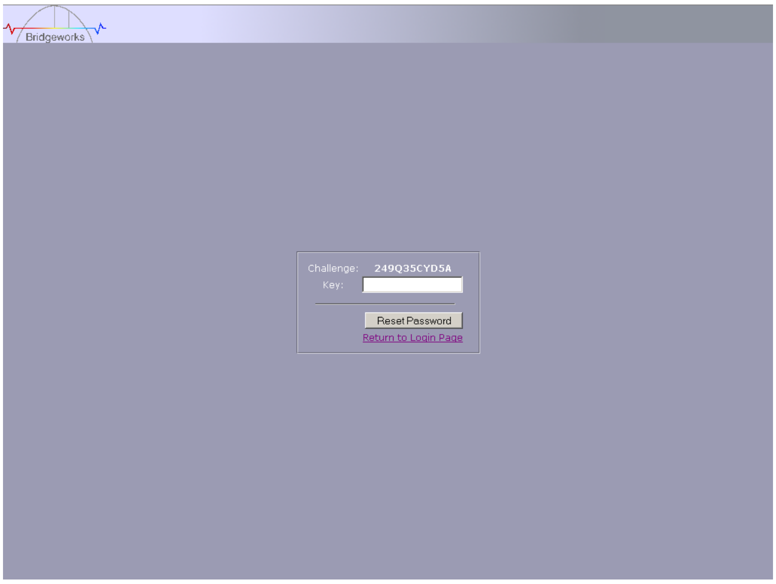
The following section describes various procedures to instigate in the event of:

- 9.1 Lost Password
- 9.2 Lost IP Address

9.1 Lost Password

If you have lost the admin password it is possible to reset it with help from Bridgeworks.

First ensure that there is nothing entered into the user field and then type **PASSWORDRESET** into the password field.



Challenge: 249Q35CYD5A

Key:

The Password Recovery Window

The unit will respond with a challenge key.

Copy this key into an email along with your name, company and contact details – you must include your company's personal email address for security purposes.

Send this email to support@4bridgeworks.com and a key will be returned for you to enter into the key field.

Press the reset button once you have entered the key – this will reset the admin user password back to admin.

9.2 Lost IP Address

Introduction

The utility will find any Bridgeworks device irrespective of its IP address; this can be helpful in determining the IP address of a Bridgeworks device with an unknown IP address and for checking the number of Bridgeworks devices on a network.

Downloading LAN Scan

The utility can be downloaded from:

http://www.4bridgeworks.com/support/software.shtml

How to use LAN Scan

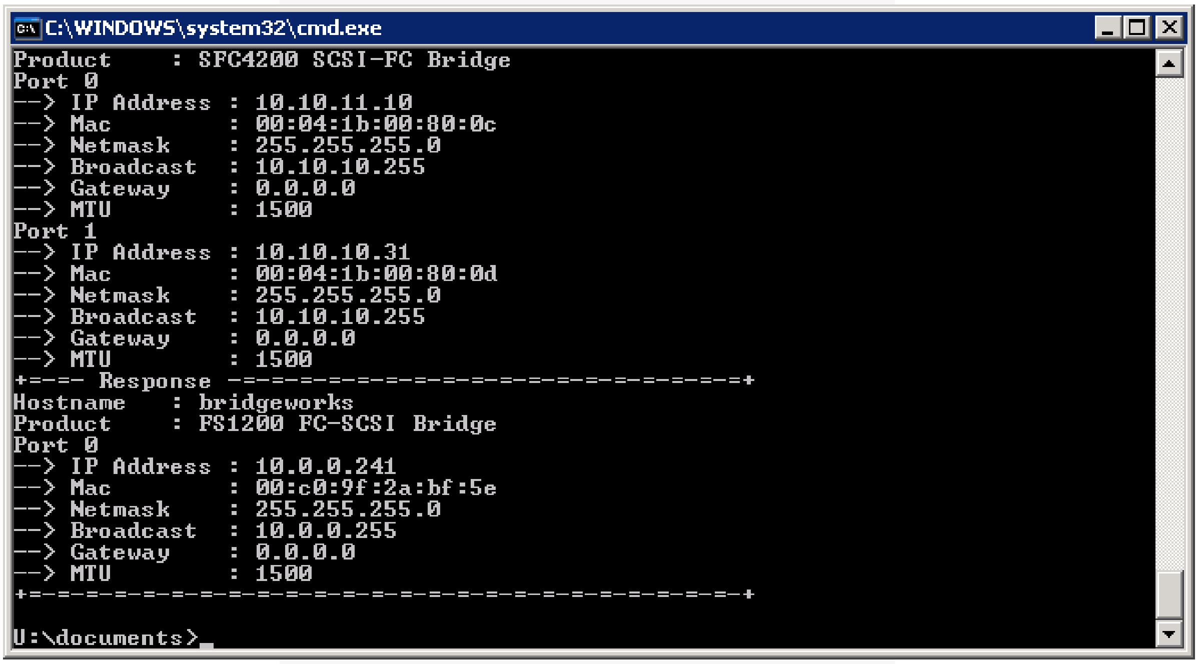
The utility is available under both Windows and Linux, and is a CLI based tool.
The downloaded file is in .zip format and contains the files lanscan, lanscan.exe and lanscan.bat.

For the GNU/Linux operating system the lanscan executable is needed.
For the Windows operating system the lanscan.exe and lanscan.bat are required

Linux
Execute lanscan within a console and the output is displayed on screen.

Windows
Double click on lanscan.bat. This will create a file named lanscan.txt. Open lanscan.txt within a text editor to view the discovered Bridgeworks devices.

Typical output



```
Product     : SFC4200 SCSI-FC Bridge
Port 0
--> IP Address : 10.10.11.10
--> Mac        : 00:04:1b:00:80:0c
--> Netmask    : 255.255.255.0
--> Broadcast  : 10.10.10.255
--> Gateway    : 0.0.0.0
--> MTU        : 1500
Port 1
--> IP Address : 10.10.10.31
--> Mac        : 00:04:1b:00:80:0d
--> Netmask    : 255.255.255.0
--> Broadcast  : 10.10.10.255
--> Gateway    : 0.0.0.0
--> MTU        : 1500
+=-=- Response -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=+
Hostname    : bridgeworks
Product     : FS1200 FC-SCSI Bridge
Port 0
--> IP Address : 10.0.0.241
--> Mac        : 00:c0:9f:2a:bf:5e
--> Netmask    : 255.255.255.0
--> Broadcast  : 10.0.0.255
--> Gateway    : 0.0.0.0
--> MTU        : 1500
+=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-+

U:\documents>_
```

Command Prompt with the Contents of LAN Scan

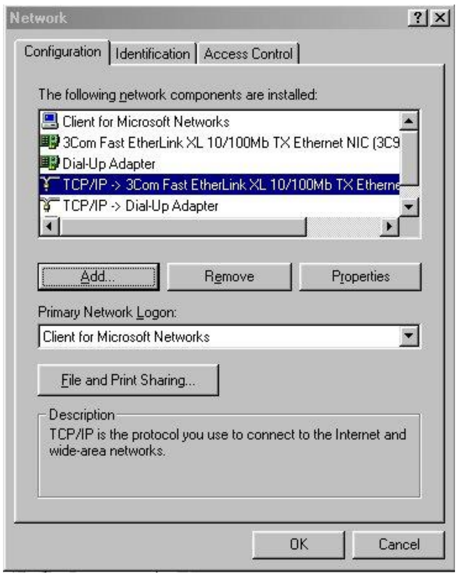
Appendix A Setting up your computer for initial set up

A1 Windows 95, 98 or NT

If your computer is running Windows 95, 98 or NT follow the instructions below .For users with Windows 2000, 2003 or XP, instructions are detailed in Appendix A2 and Windows Server 2008, 7 or Vista, instructions are detailed in Appendix A3.

From the **Start** menu, choose **Settings** then **Control Panel**.

Then click the **Network** icon



The following network components are installed:

- Client for Microsoft Networks
- 3Com Fast EtherLink XL 10/100Mb TX Ethernet NIC (3C9
- Dial-Up Adapter
- TCP/IP -> 3Com Fast EtherLink XL 10/100Mb TX Etherne
- TCP/IP -> Dial-Up Adapter

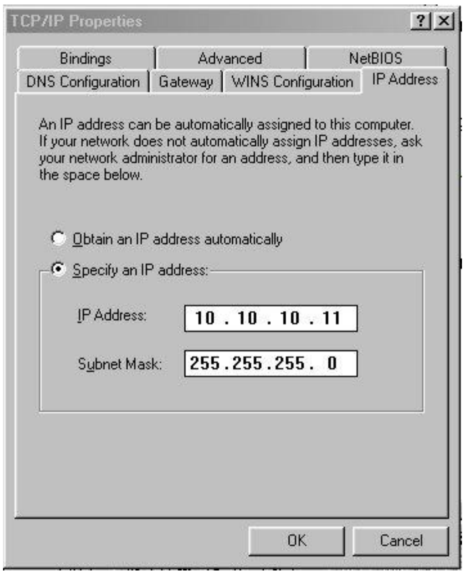
Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

In the **Network** window's **Configuration** tab,

Select the **TCP/IP** entry

Then the **Properties** Button



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 10 . 10 . 10 . 11

Subnet Mask: 255 . 255 . 255 . 0

Click on the **IP Address** tab

Make a note of your current set up then:

Click on the **Specify an IP** address button

Enter **10.10.10.11**into the **IP Address** field

Enter **255.255.255.0** into the **Subnet Mask** field

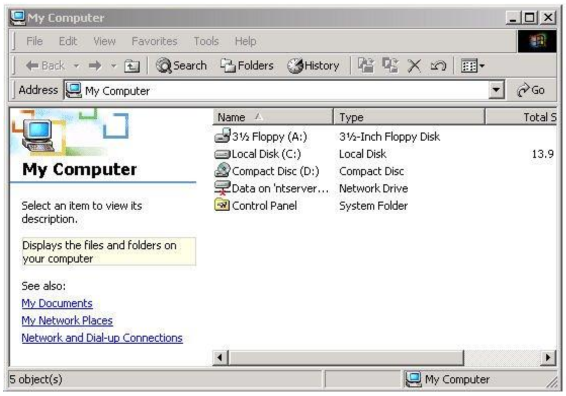
Finally click the OK button and reboot your computer.

Note: Once you have completed the initial set up of the Node, return your computer to the original settings and reconnect to the Node.

A2 Windows 2000, 2003 or XP

If your computer is running Windows, 2000, 2003 or XP follow the instructions below .For users with Windows 95, 98 or NT instructions are detailed in Appendix A1 and Windows Server 2008, 7 or Vista, instructions are detailed in Appendix A3.

From the **Desk Top** or **Start** menu, select **My Computer**


My Computer
File Edit View Favorites Tools Help
Back Search Folders History
Address My Computer
Go

My Computer

Select an item to view its description.

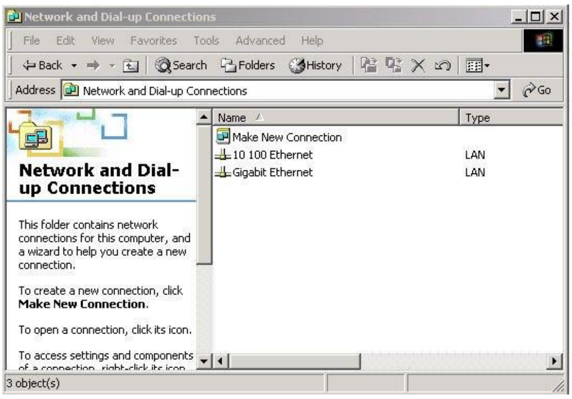
Displays the files and folders on your computer

See also:
My Documents
My Network Places
Network and Dial-up Connections

Name	Type	Total S
3½ Floppy (A:)	3½-Inch Floppy Disk	
Local Disk (C:)	Local Disk	13.9
Compact Disc (D:)	Compact Disc	
Data on 'ntserver…	Network Drive	
Control Panel	System Folder	

5 object(s) My Computer

In the My Computer window select **Network and Dial-up Connections** positioned in the bottom left hand corner


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go

Network and Dial-up Connections

This folder contains network connections for this computer, and a wizard to help you create a new connection.

To create a new connection, click **Make New Connection**.

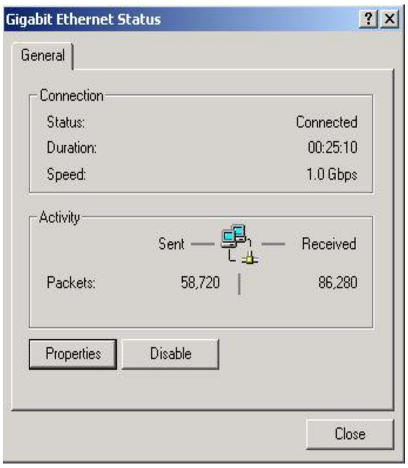
To open a connection, click its icon.

To access settings and components of a connection, right-click its icon.

Name	Type
Make New Connection	
10 100 Ethernet	LAN
Gigabit Ethernet	LAN

3 object(s)

From within the displayed **Network and Dial-up Connections** select the interface connection that will be used to connect to the iSCSI Node – in this example we have selected the Gigabit Ethernet interface.



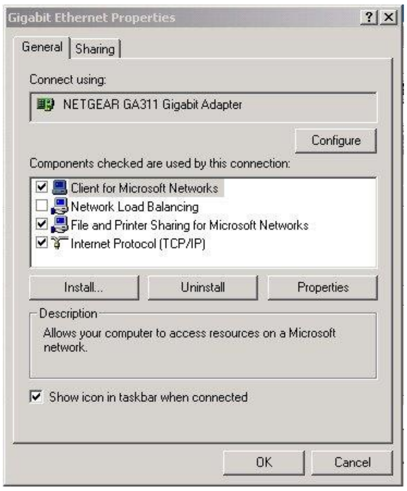
Connection

Status: Connected
Duration: 00:25:10
Speed: 1.0 Gbps

Activity

Sent — Received
Packets: 58,720 | 86,280

A general status page will be displayed. From within this page select **Properties**



Gigabit Ethernet Properties

Connect using:

NETGEAR GA311 Gigabit Adapter

Components checked are used by this connection:

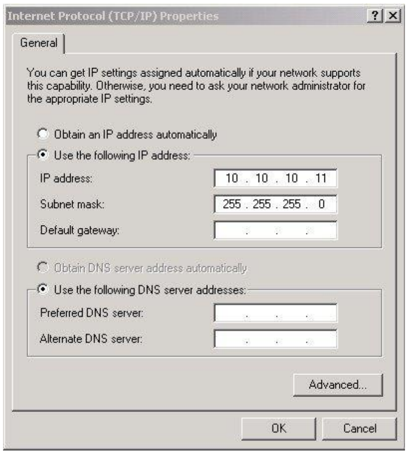
- ☑ Client for Microsoft Networks
- ☐ Network Load Balancing
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in taskbar when connected

Select the **Internet Protocol** (TCP/IP) entry and then **Properties**



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Make a note of your current set up then:

Click **Use the following IP Address**

Enter **10.10.10.11** into the **IP Address** field

Enter **255.255.255.0** into the **Subnet Mask** field

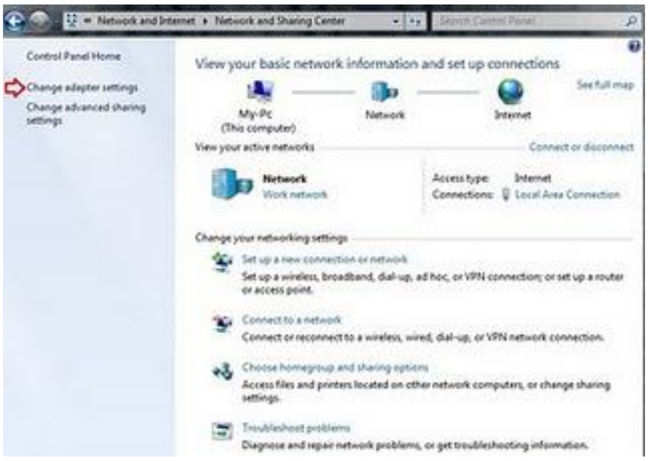
Finally click the OK button.

Note: Once you have completed the initial set up of the Node, return your computer to the original settings and reconnect to the Node.

A3 Windows Vista, Server 2008 or 7

If your computer is running Windows, Vista or 7 follow the instructions below .For users with Windows 95, 98 or NT instructions are detailed in Appendix A1 and Windows 2000, 2003 or XP, instructions are detailed in Appendix A2.

From the **Start** menu, select **Control panel**



View your basic network information and set up connections

View your active networks

Network

Access type: Internet

Connections: Local Area Connection

Change your networking settings

Set up a new connection or network

Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options

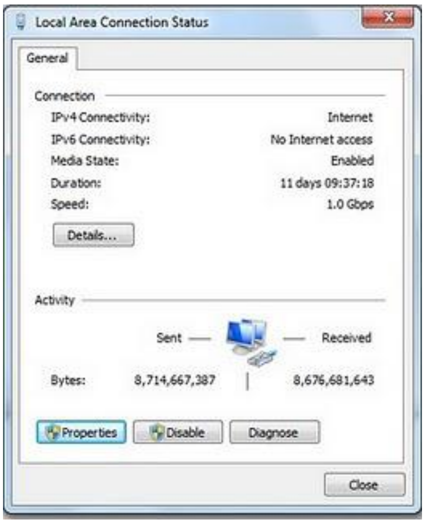
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

From the control panel select the **Network and Internet link**, followed by the **Network and Sharing Centre link**.

Now you can see **Local Area connection** dialogue box. Double click Local Area Connections.



Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 11 days 09:37:18

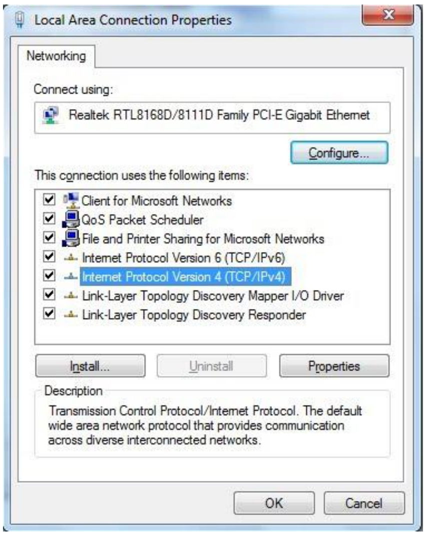
Speed: 1.0 Gbps

Activity

Sent — — Received

Bytes: 8,714,667,387 | 8,676,681,643

A general status page will be displayed. From with in this page select **Properties**



Connect using:

Realtek RTL8168D/8111D Family PCI-E Gigabit Ethernet

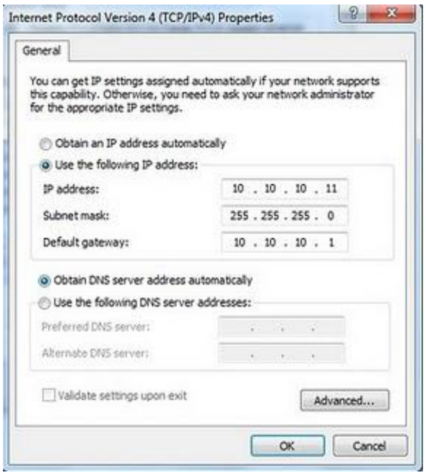
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Select the **Internet Protocol Version 4** (TCP/IP) entry and then **Properties**



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 10 . 10 . 1

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Make a Note of your current set up then:

Click **Use the following IP Address**

Enter **10.10.10.11** into the **IP Address** field

Enter **255.255.255.0** into the **Subnet Mask** field

Finally click the OK button.

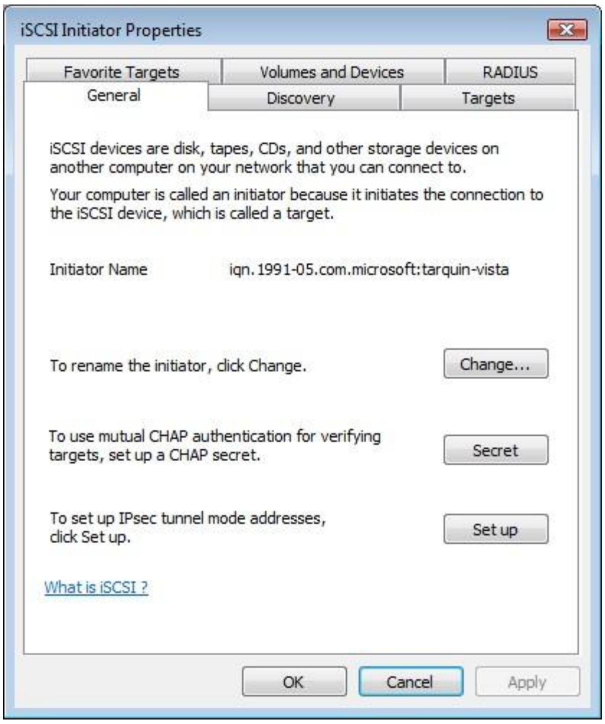
Note: Once you have completed the initial set up of the Node, return your computer to the original settings and reconnect to the Node.

Appendix B Connecting to an iSCSI Device using the Microsoft iSCSI Initiator

B1 Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows Vista Server 2008 R1 or Server 2003

There are many iSCSI Initiators available. However, for the purpose of this user guide we shall concentrate only on the Microsoft iSCSI Initiator. In this example we have used the Microsoft iSCSI that is available with Microsoft Vista. However, the following procedure should be identical for all versions of Microsoft iSCSI Initiator.

Step 1 – General Set up
Open the iSCSI initiator and then click on the General Tab. You should see a window as shown below.



iSCSI devices are disk, tapes, CDs, and other storage devices on another computer on your network that you can connect to.

Your computer is called an initiator because it initiates the connection to the iSCSI device, which is called a target.

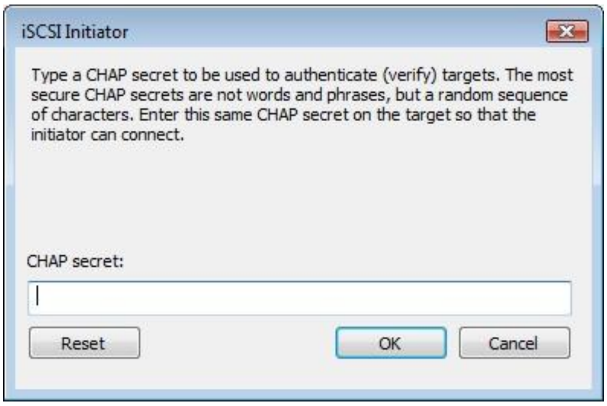
Initiator Name   iqn.1991-05.com.microsoft:tarquin-vista

To rename the initiator, click Change.

To use mutual CHAP authentication for verifying targets, set up a CHAP secret.

To set up IPsec tunnel mode addresses, click Set up.

In this window the user is able to configure the initiator name, specify the initiator secret and set up the IPsec connections. For the purpose of this document we shall leave the initiator name as the default.
If you intend to use Mutual CHAP authentication you must enter the Initiator secret on this page.
Click on the secret button and a window should be displayed



iSCSI Initiator

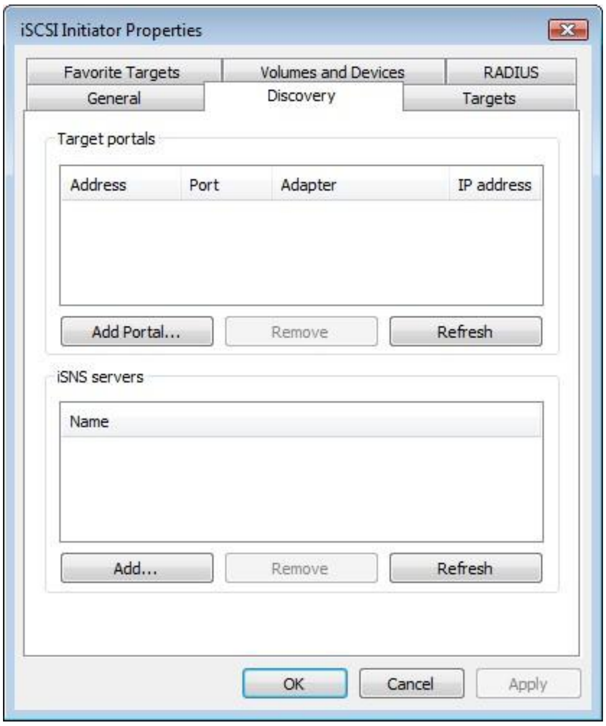
Type a CHAP secret to be used to authenticate (verify) targets. The most secure CHAP secrets are not words and phrases, but a random sequence of characters. Enter this same CHAP secret on the target so that the initiator can connect.

CHAP secret:

Enter in the Initiator Secret and click OK. The secret should be between 12 and 16 characters.
Make a note of this secret as you will need to enter this as part of configuring CHAP on the iSCSI Node

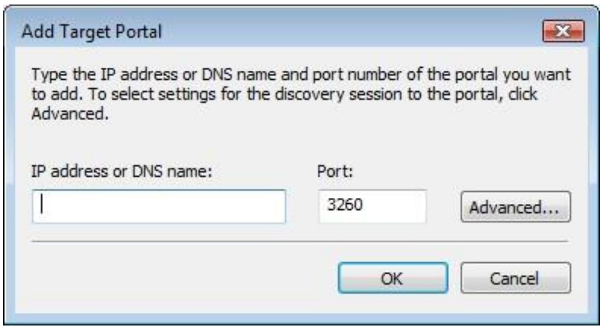
Step 2 - Discovery of Devices

Before the user can connect to an iSCSI Target, the iSCSI targets must be discovered.
Click on the Discovery tab and you should see the window below



iSCSI Initiator Properties

To add an iSCSI Target portal, click on ‘Add Portal’. The user should now be presented with a window.



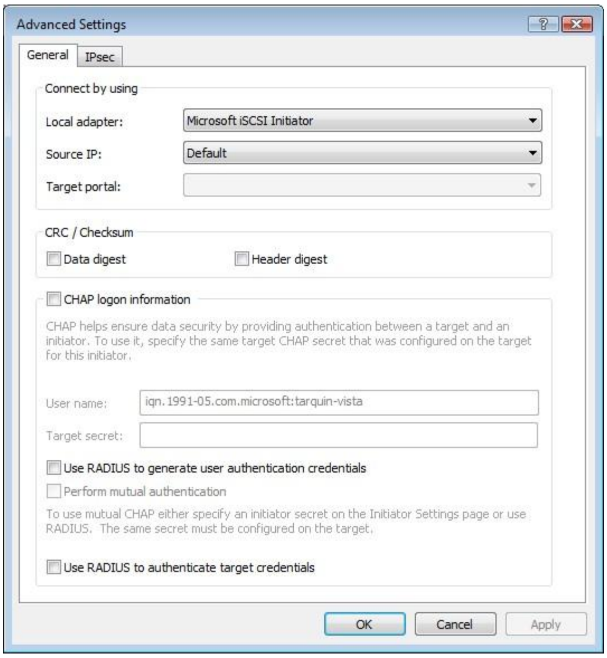
Add Target Portal

Type the IP address or DNS name and port number of the portal you want to add. To select settings for the discovery session to the portal, click Advanced.

IP address or DNS name:

Port: 3260

Enter an IP-address for the iSCSI Target. In this example we shall use the IP-address of 10.10.10.50. Leave the port 3260 unless you have configured your iSCSI Node only to respond on port 860, in which case change it to 860. Click on the advanced button to see the advanced options.



Advanced Settings

General | IPsec

Connect by using

Local adapter: Microsoft iSCSI Initiator

Source IP: Default

Target portal:

CRC / Checksum

□ Data digest □ Header digest

□ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.

User name: iqn.1991-05.com.microsoft:tarquin-vista

Target secret:

□ Use RADIUS to generate user authentication credentials

□ Perform mutual authentication

To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.

□ Use RADIUS to authenticate target credentials

The ‘Connect by using‘ box allows the user to specify which iSCSI Adaptor to use and the Source IP. The Local adaptor will only differ from Microsoft iSCSI Initiator setting if an iSCSI Offload card has been installed. For the purpose of this guide we shall only use the Microsoft iSCSI Initiator. Leaving this setting as Default will also use the Microsoft iSCSI Initiator.

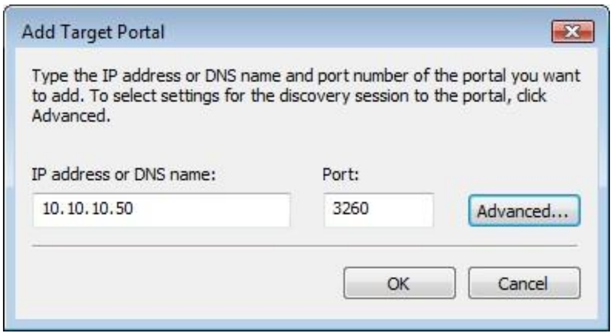
The Source IP is used to specify upon which network adaptor the discovery will be done. In most cases the user will want to leave this as default. If multiple network interfaces are installed in the Server and the user wishes to select a particular interface, select the IP-address of that network interface from the pull down list.

CRC/Checksum settings allow the user to specify whether the discovery is done using Data and/or Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended then Header and Data Digests are left disabled, as performance will be affected.

If the iSCSI Node has had CHAP enabled, or the user wishes to authenticate the iSCSI Node, click on the checkbox ‘CHAP login information’ to enable CHAP. Now enter the username and target secret that was configured on the iSCSI Node. If the user wishes to authenticate the iSCSI Node, select ‘Perform mutual authentication’.

Note: For mutual CHAP to be performed, the Initiator Secret must be set on the general tab, and be the same as the one configured on the iSCSI Node.

The use of RADUS is beyond the scope of this guide.
Once the user is satisfied that all advanced options are correct click OK.
The user should now see a window as below.



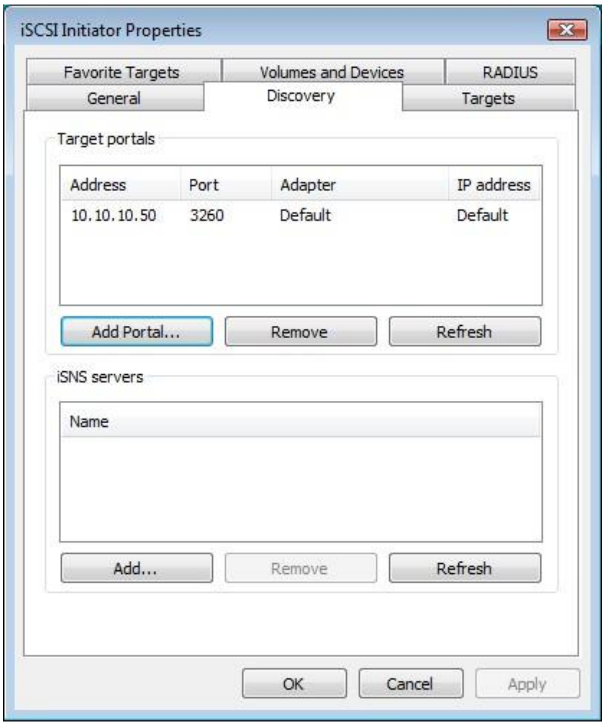
Add Target Portal

Type the IP address or DNS name and port number of the portal you want to add. To select settings for the discovery session to the portal, click Advanced.

IP address or DNS name: 10.10.10.50

Port: 3260

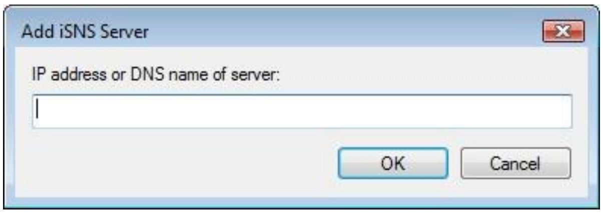
Now click OK and the Microsoft iSCSI Initiator shall perform the discovery. This usually performs quickly but can take up to a minute with multiple network ports.
Once the discovery is complete, the user should see the target listed in the Target Portals list. .



iSCSI Initiator Properties

Address	Port	Adapter	IP address
10.10.10.50	3260	Default	Default

If the user has an iSNS-server then the address can be added in the iSNS-servers list by clicking Add.
A window should appear

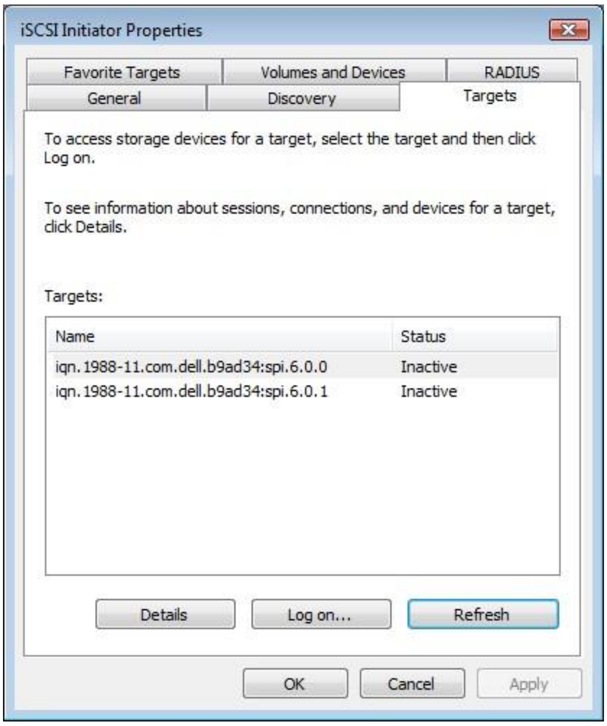


Add iSNS Server

IP address or DNS name of server:

Enter the address of the iSNS-Server then click OK. The Microsoft iSCSI-Initiator will now query the iSNS-Server and discover any iSCSI-Targets that are registered.

Step 3 – Targets
Click on the Targets tab.
The devices discovered should now be listed and shown as below



To access storage devices for a target, select the target and then click Log on.

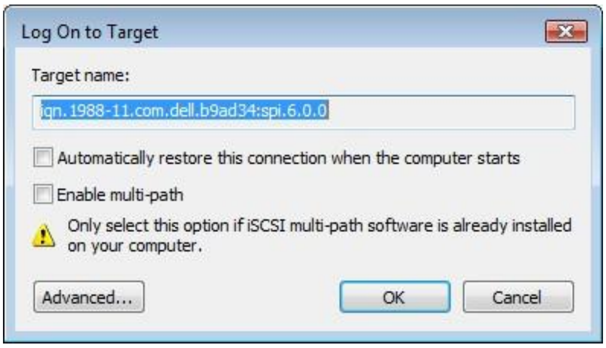
To see information about sessions, connections, and devices for a target, click Details.

Targets:

Name	Status
iqn.1988-11.com.dell.b9ad34:spi.6.0.0	Inactive
iqn.1988-11.com.dell.b9ad34:spi.6.0.1	Inactive

In this example two iSCSI targets have been discovered. The first device is the tape drive, and the second is the media changer. If no devices are displayed, check the settings used to do the discovery, especially the CHAP settings then return to Targets tab and click Refresh. If still no devices are displayed, check network cables and that the iSCSI Node is operational.

To connect to one of the iSCSI Targets, click on one of the target names and then click the 'Log on' button. In this example we have chosen the first target. A window should appear.



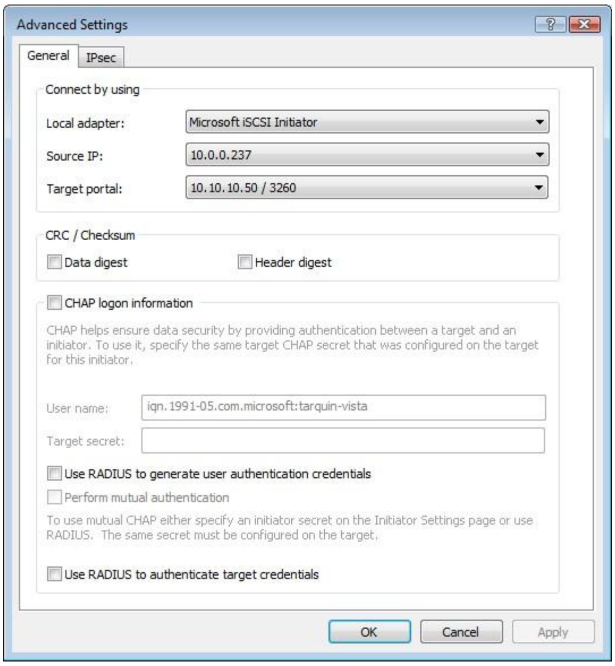
Target name:
iqn.1988-11.com.dell.b9ad34:spi.6.0.0

□ Automatically restore this connection when the computer starts

□ Enable multi-path

⚠ Only select this option if iSCSI multi-path software is already installed on your computer.

If the user wishes to connect to the target automatically when the computer is booted, click the checkbox 'Automatically restore this connection when the computer starts'.
Even if the user wishes to connect to the iSCSI Target using multi-path, they should not check 'Enable multi-path' Checkbox. This will be covered in a following section.
Now click on the advanced button to see the advanced settings. A window should appear as below.



Connect by using

Local adapter: Microsoft iSCSI Initiator

Source IP: 10.0.0.237

Target portal: 10.10.10.50 / 3260

CRC / Checksum

□ Data digest □ Header digest

□ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.

User name: iqn.1991-05.com.microsoft:tarquin-vista

Target secret:

□ Use RADIUS to generate user authentication credentials

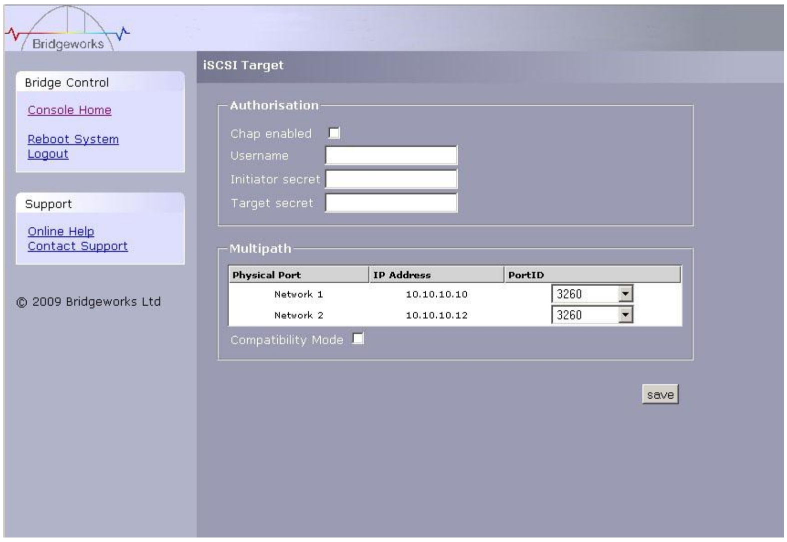
□ Perform mutual authentication

To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.

□ Use RADIUS to authenticate target credentials

This advanced settings page is the same as that of the discovery with one addition. On the ‘Connect by using’ section the user can select the Target Port that he wishes to connect too. This is particularly useful if the user is going to create multiple connections. In this example we have chosen to connect to the IP-address 10.10.10.50 on port 3260.

To see how this relates to the iSCSI Node configuration note the IP-addresses in the window shown below.



© 2009 Bridgeworks Ltd

iSCSI Target

Authorisation

Chap enabled □

Username

Initiator secret

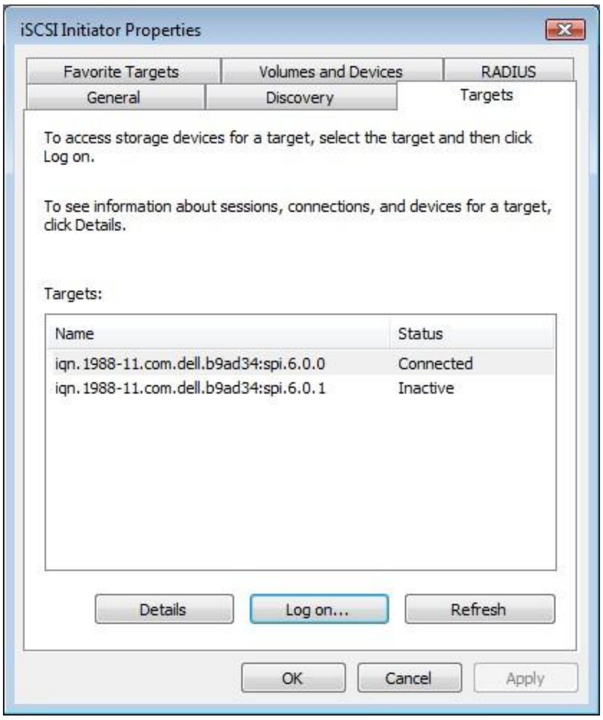
Target secret

Multipath

Physical Port	IP Address	PortID
Network 1	10.10.10.10	3260
Network 2	10.10.10.12	3260

Compatibility Mode □

Set up the Digest and CHAP settings as described in stage 2 during the discovery phase and click OK. This will now take you back to the window that was shown previously. Click OK once more. The user should now see the iSCSI Target connected.



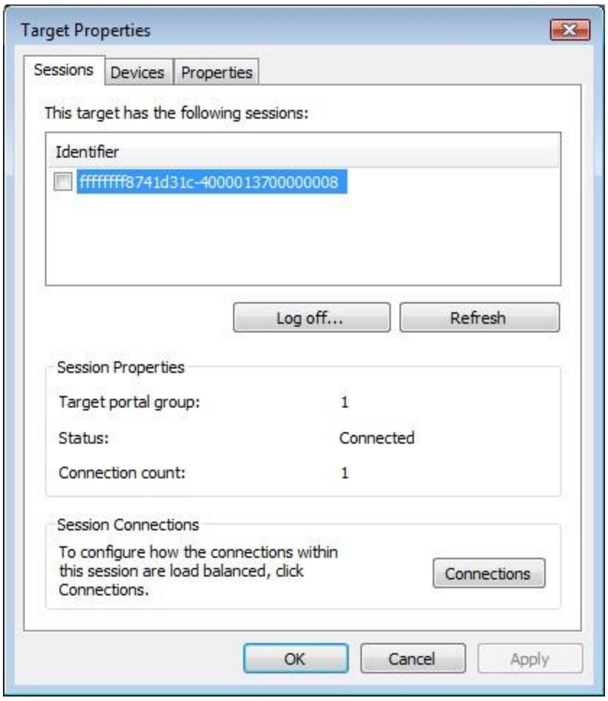
To access storage devices for a target, select the target and then click Log on.

To see information about sessions, connections, and devices for a target, click Details.

Targets:

Name	Status
iqn.1988-11.com.dell.b9ad34:spi.6.0.0	Connected
iqn.1988-11.com.dell.b9ad34:spi.6.0.1	Inactive

Step 4 – Viewing iSCSI Session Details
Now that the user has connected to an iSCSI Target, to check that the device is connected click on the Details button. A window should appear.



This target has the following sessions:

Identifier
□ ffffffff8741d31c-4000013700000008

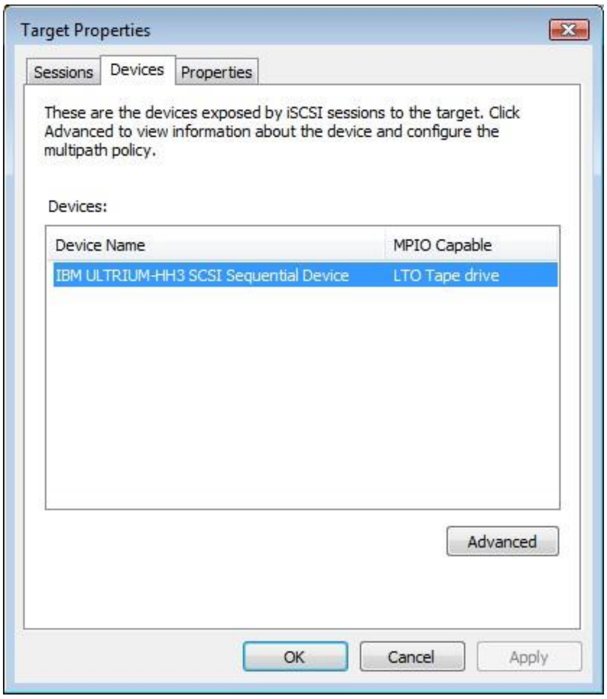
Session Properties

Target portal group:	1
Status:	Connected
Connection count:	1

Session Connections

To configure how the connections within this session are load balanced, click Connections.

In this window the user can view the iSCSI Sessions associated to the iSCSI Target, how many connections are attached to each iSCSI Session, and the Target Portal Group. If the user clicks on the Device tab, he should see details of the target device. Here we can see that the device is an IBM LTO Tape drive.

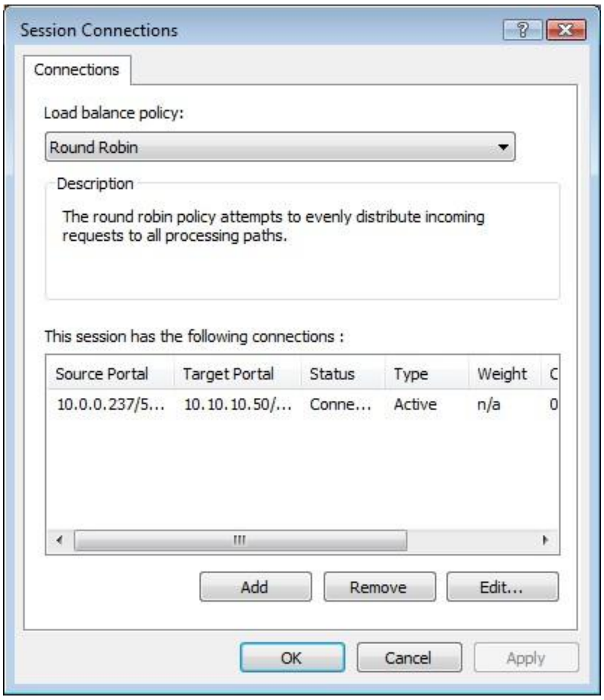


These are the devices exposed by iSCSI sessions to the target. Click Advanced to view information about the device and configure the multipath policy.

Devices:

Device Name	MPIO Capable
IBM ULTRIUM-HH3 SCSI Sequential Device	LTO Tape drive

Step 5 – Creating multiple connections (Optional)
If the user wishes to create multiple connections to an iSCSI Session, return to the Session tab in the Target Properties window.
Click on the Connections button and a window should appear. This is shown below.



Load balance policy: Round Robin

Description

The round robin policy attempts to evenly distribute incoming requests to all processing paths.

This session has the following connections :

Source Portal	Target Portal	Status	Type	Weight	C
10.0.0.237/5...	10.10.10.50/...	Conne...	Active	n/a	0

The Session Connections window shows how many iSCSI Connections are active and the type of load balance used. For all iSCSI Sessions there will be at least one 'leading connection'.

iSCSI connections can be added and removed at any time, all apart from the leading connection, which can only be removed when the iSCSI Session is logged off.

The Load balance policy specifies how the data is distributed over multiple connections. The main policies that should be used are ‘Round Robin’ and ‘Fail Over Only’.

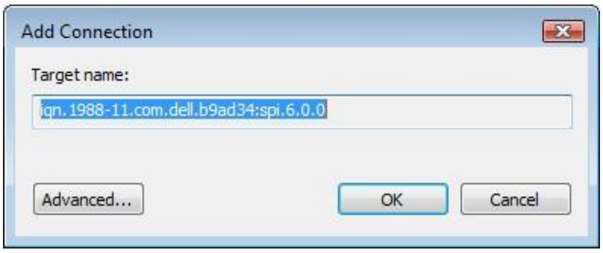
Round Robin will utilize all connections for data and evenly distribute the data.

Fail Over Only will use the Leading connection for data transfer. If a connection should go down then the data transfer shall switch on one of the other connections.

For most purposes Round Robin will provide the greatest performance increase.

If you have been experiencing a performance decrease when transferring data to more than one device using multiple connections, please refer to the trouble-shooting guide.

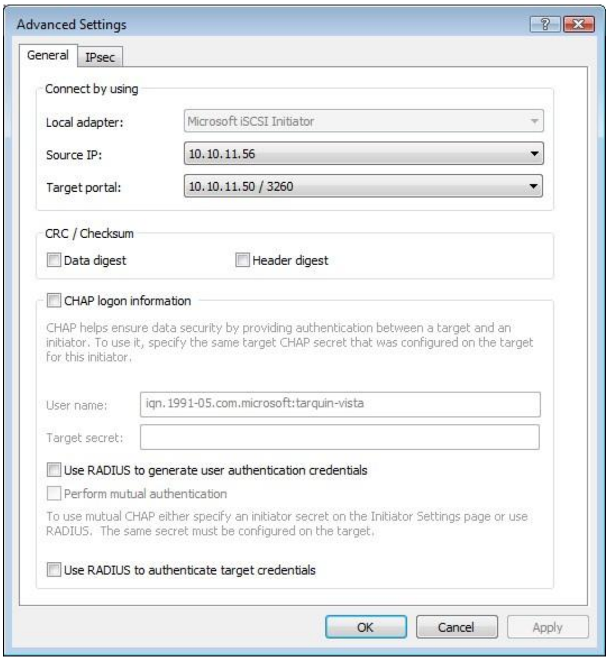
To add a new connection to a session, click on the Add button and a new window should appear.



Add Connection

Target name: iqn.1988-11.com.dell.b9ad34:spi.6.0.0

Now click on the 'Advanced' button to see the Advanced Settings.



Advanced Settings

General | IPsec

Connect by using

Local adapter: Microsoft iSCSI Initiator

Source IP: 10.10.11.56

Target portal: 10.10.11.50 / 3260

CRC / Checksum

□ Data digest □ Header digest

□ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.

User name: iqn.1991-05.com.microsoft:tarquin-vista

Target secret:

□ Use RADIUS to generate user authentication credentials

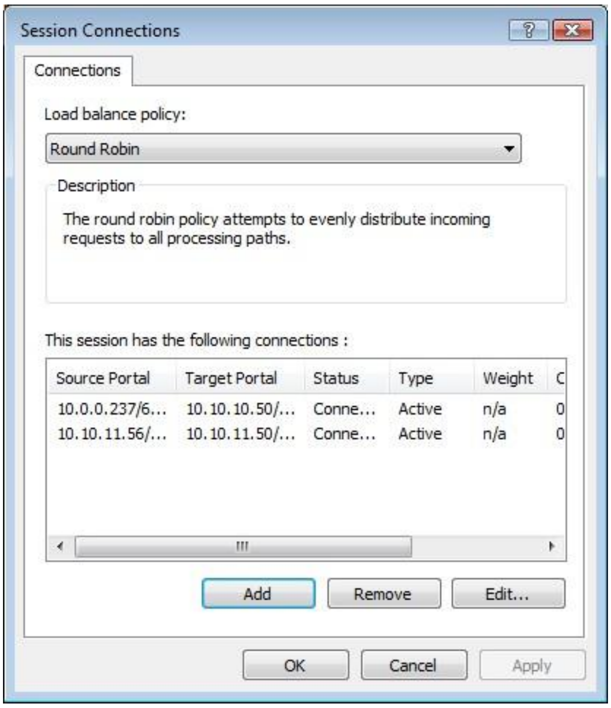
□ Perform mutual authentication

To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.

□ Use RADIUS to authenticate target credentials

Select the Source IP-address and the Target Portal that you wish to connect too via the pull down menus in the “Connect by using” section. When setting up multiple connections you ideally want to connect to different ports and different network interfaces. In this example we have connected to 10.10.10.50/3260 as the leading connection and the second connection will be 10.10.11.50/3260.

Set up CHAP and Digest then click OK. The user will now be brought back to the window below. Click OK and now the user should see the Session Connections page with two connections.



Load balance policy: Round Robin

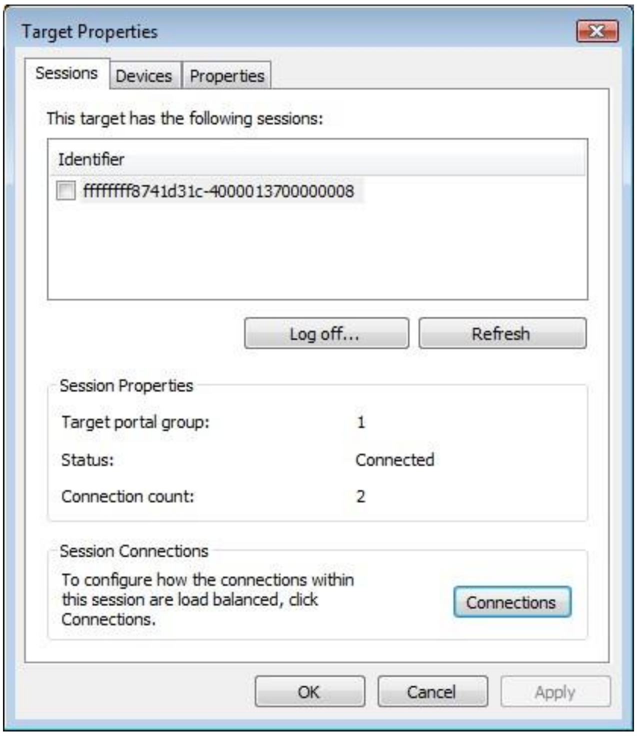
Description

The round robin policy attempts to evenly distribute incoming requests to all processing paths.

This session has the following connections :

Source Portal	Target Portal	Status	Type	Weight	C
10.0.0.237/6...	10.10.10.50/...	Conne...	Active	n/a	0
10.10.11.56/...	10.10.11.50/...	Conne...	Active	n/a	0

The user can add up to 8 different connections.
Once the user has completed setting up the connections, click OK to return to the iSCSI session page. You should now see the number of connections increased. In this example we have 2 connections.



This target has the following sessions:

Identifier
□ ffffffff8741d31c-4000013700000008

Session Properties

Target portal group: 1

Status: Connected

Connection count: 2

Session Connections

To configure how the connections within this session are load balanced, click Connections.

Now click on OK to return to the Microsoft iSCSI Initiator main window.

Step 6 – Logging off an iSCSI Session
To log off an iSCSI Session, follow the following procedure.

- Open the Microsoft iSCSI Initiator and click on the Targets tab.

- Click on the iSCSI session that the user wishes to log off and then click Details.
- In the Target Properties window, select the Sessions Tab and select the identifier that is to be logged off.
- Click the Log off button. This will log off all connections associated with the iSCSI Session.

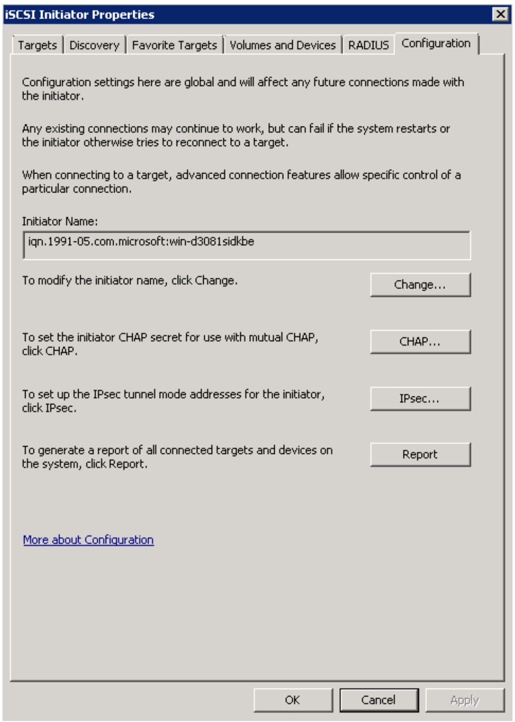
The session identifier should now be removed from the identifier list. Click ok to return to the main iSCSI Initiator window. The iSCSI device should now show as inactive.

B2 Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows Server 2008 R2

There are many iSCSI initiators available. For the purpose of this user guide we shall concentrate only on the Microsoft iSCSI Initiator. In this example we have used the Microsoft iSCSI that is available with Microsoft Server 2008 R2.

Step 1 – General Set up

Open the iSCSI initiator and then click on the Configuration Tab. You should see a window as shown below.



Configuration settings here are global and will affect any future connections made with the initiator.

Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.

When connecting to a target, advanced connection features allow specific control of a particular connection.

Initiator Name: iqn.1991-05.com.microsoft:win-d3081sidkbe

To modify the initiator name, click Change.

To set the initiator CHAP secret for use with mutual CHAP, click CHAP.

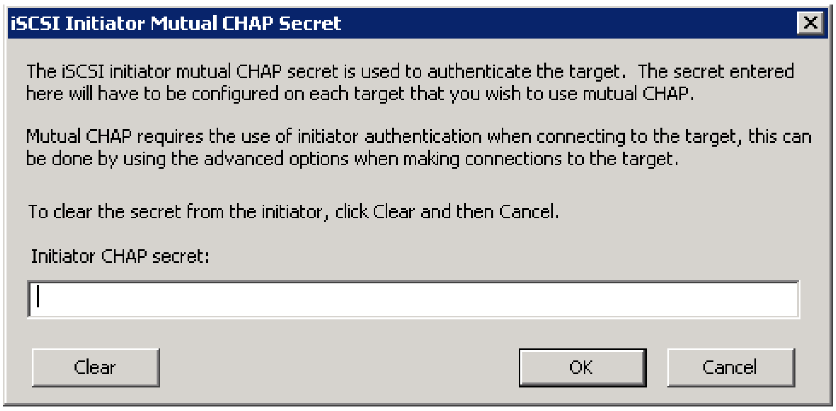
To set up the IPsec tunnel mode addresses for the initiator, click IPsec.

To generate a report of all connected targets and devices on the system, click Report.

In this window the user is able to configure the initiator name, specify the initiator secret and set up the IPsec connections. For the purpose of this document we shall leave the initiator name as the default.

If you intend to use Mutual CHAP authentication you must enter the initiator secret on this page.

Click on the secret button and a window should be displayed



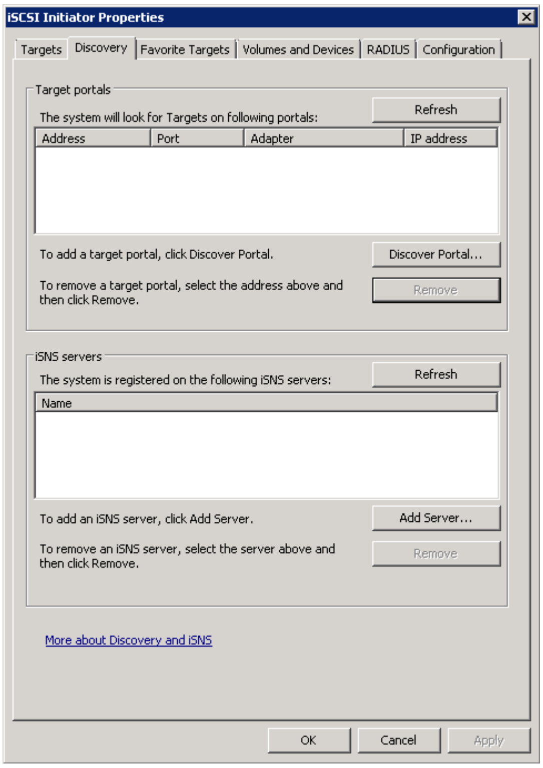
The iSCSI initiator mutual CHAP secret is used to authenticate the target. The secret entered here will have to be configured on each target that you wish to use mutual CHAP.

Mutual CHAP requires the use of initiator authentication when connecting to the target, this can be done by using the advanced options when making connections to the target.

To clear the secret from the initiator, click Clear and then Cancel.

Enter in the initiator secret and click OK. The secret should be between 12 and 16 characters.
Make a note of this secret, as you will need to enter this as part of configuring CHAP on the iSCSI Node.

Step 2 - Discovery of Devices
Before the user can connect to an iSCSI Target, the targets must be discovered.
Click on the Discovery tab and you should see the window below



The system will look for Targets on following portals:

To add a target portal, click Discover Portal.

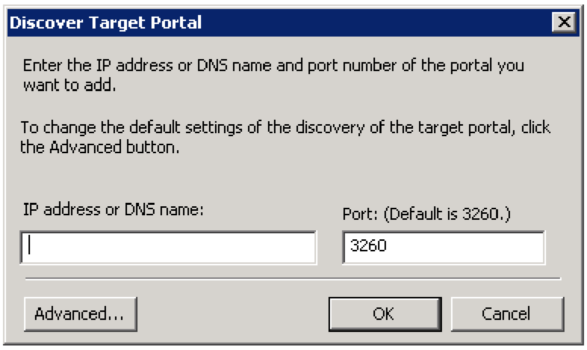
To remove a target portal, select the address above and then click Remove.

The system is registered on the following iSNS servers:

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

To add an iSCSI Target portal, click on ‘Discover Portal’. The user should now be presented with a window.


Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

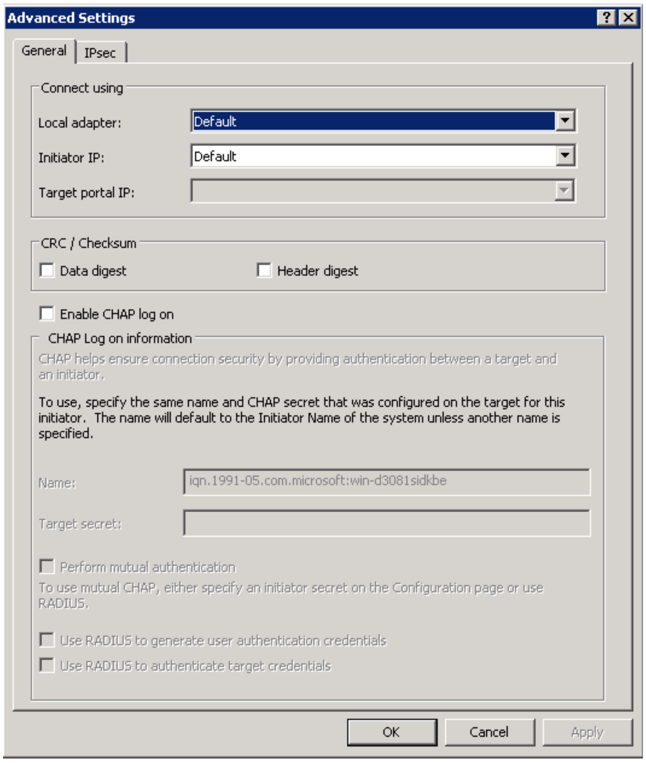
To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name:

Port: (Default is 3260.) 3260

Enter an IP-address for the iSCSI Target. In this example we shall use the IP-address of 10.10.10.99.

Leave the port 3260 unless you have configured your iSCSI Node only to respond on port 860, in which case change it to 860. Click on the advanced button to see the advanced options.


Advanced Settings

Connect using

Local adapter: Default

Initiator IP: Default

Target portal IP:

CRC / Checksum

□ Data digest □ Header digest

□ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:win-d3081sidkbe

Target secret:

□ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

The ‘Connect using‘ box allows the user to specify which iSCSI Adaptor to use and the Source IP. The Local adaptor will only differ from Microsoft iSCSI Initiator setting if an iSCSI Offload card has been installed. For the purpose of this guide we shall only use the Microsoft iSCSI Initiator. Leaving this setting as default will also use the Microsoft iSCSI Initiator.

The Initiator IP is used to specify upon which network adaptor the discovery will be done. In most cases the user will want to leave this as default. If multiple network interfaces are installed in the server and the user wishes to select a particular interface, select the IP-address of that network interface from the pull down list.

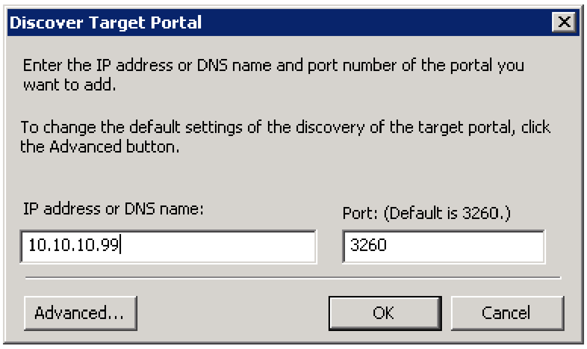
CRC/Checksum settings allow the user to specify whether the discovery is done using Data and/or Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended that Header and Data Digests are left disabled, as performance will be affected.

If the iSCSI Node has had CHAP enabled, or the user wishes to authenticate the iSCSI Node, click on the checkbox ‘Enable CHAP log on’ to enable CHAP. Now enter the username and target secret that was configured on the iSCSI Node. If the user wishes to authenticate the iSCSI Node, select ‘Perform mutual authentication’.

Note: For mutual CHAP to be performed, the Initiator Secret must be set on the general tab, and be the same as the one configured on the iSCSI Node.

The use of RADUS is beyond the scope of this guide.

Once the user is satisfied that all advanced options are correct click OK.
The user should now see a window as below.



Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

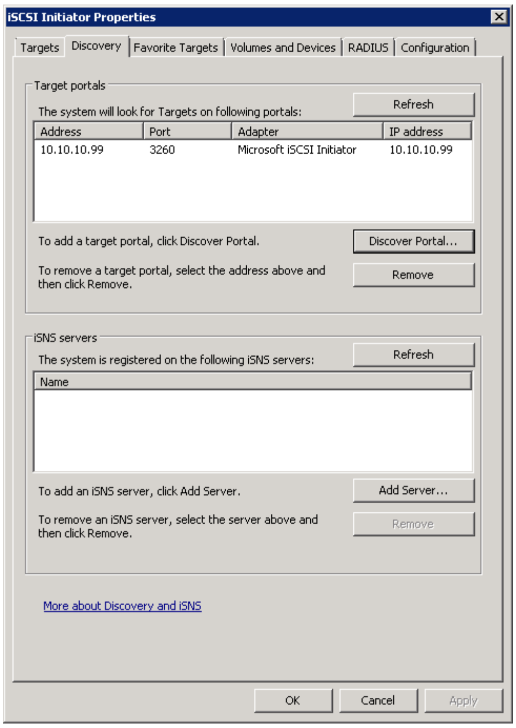
To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: 10.10.10.99

Port: (Default is 3260.) 3260

Now click OK and the Microsoft iSCSI Initiator shall perform the discovery. This usually performs quickly but can take up to a minute with multiple network ports.

Once the discovery is complete, the user should see the target listed in the Target Portals list.



iSCSI Initiator Properties

Target portals

The system will look for Targets on following portals:

Address	Port	Adapter	IP address
10.10.10.99	3260	Microsoft iSCSI Initiator	10.10.10.99

To add a target portal, click Discover Portal.

To remove a target portal, select the address above and then click Remove.

iSNS servers

The system is registered on the following iSNS servers:

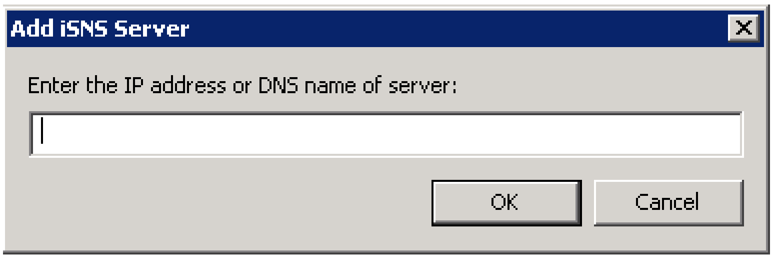
Name

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

More about Discovery and iSNS

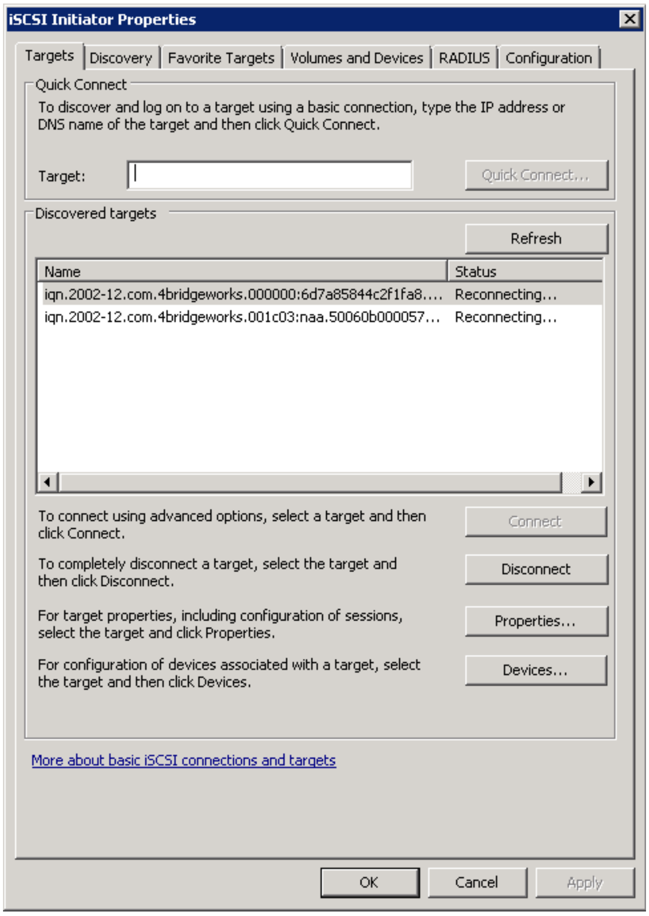
If the user has an iSNS-server then the address can be added in the iSNS-servers list by clicking ‘Add Server’. A window should appear.


Add iSNS Server

Enter the IP address or DNS name of server:

Enter the address of the iSNS-Server then click OK. The Microsoft iSCSI-Initiator will now query the iSNS-Server and discover any iSCSI-Targets that are registered.

Step 3 – Targets
Click on the Targets tab.
The devices discovered should now be listed and shown as below


iSCSI Initiator Properties

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.2002-12.com.4bridgeworks.000000:6d7a85844c2f1fa8....	Reconnecting...
iqn.2002-12.com.4bridgeworks.001c03:naa.50060b000057...	Reconnecting...

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

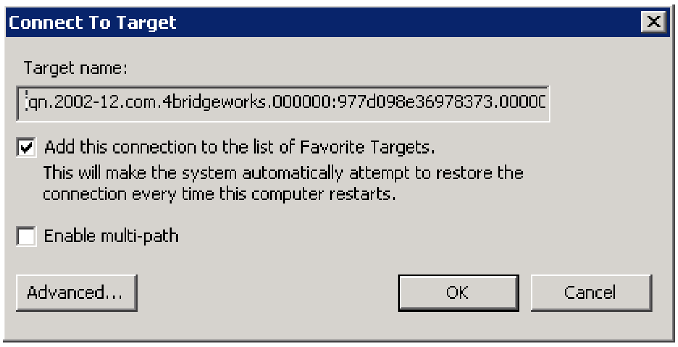
For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

More about basic iSCSI connections and targets

In this example two iSCSI targets have been discovered. The first device is the tape drive, and the second is the media changer. If no devices are displayed, check the settings used to do the discovery, especially the CHAP settings then return to Targets tab and click Refresh. If still no devices are displayed, check network cables and that the iSCSI Node is operational.

To connect to one of the iSCSI Targets, click on one of the target names and then click the ‘Log on’ button. A window should appear.



Connect To Target

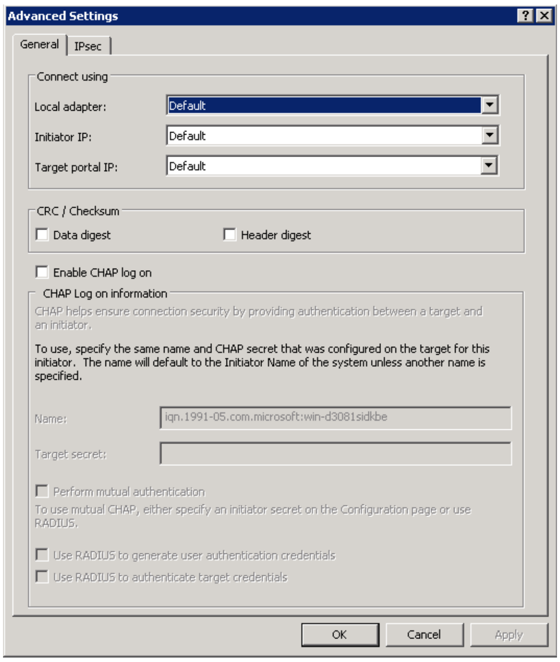
Target name:

:qn.2002-12.com.4bridgeworks.000000:977d098e36978373.0000C

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

☐ Enable multi-path

Even if the user wishes to connect to the iSCSI Target using multi-path, they should not check ‘Enable multi-path’ Checkbox. This will be covered in a following section.
Now click on the advanced button to see the advanced settings. A window should appear as below.



Advanced Settings

Connect using

Local adapter: Default

Initiator IP: Default

Target portal IP: Default

CRC / Checksum

☐ Data digest ☐ Header digest

☐ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:win-d3081sidkbe

Target secret:

☐ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

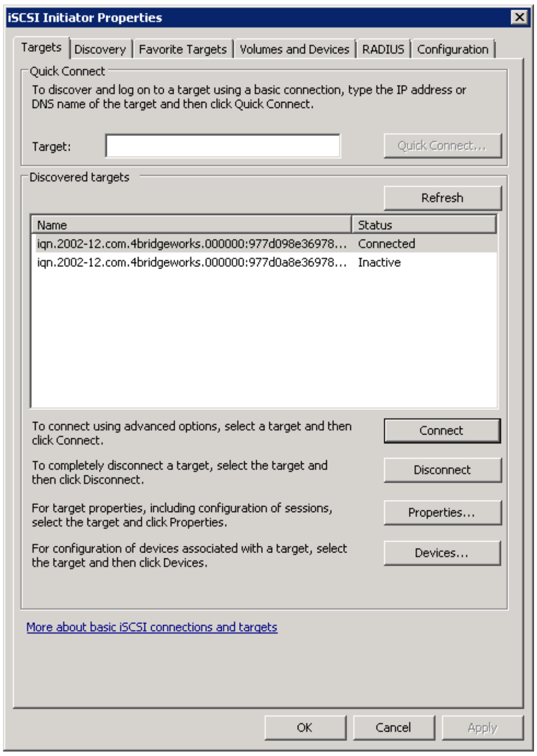
☐ Use RADIUS to generate user authentication credentials

☐ Use RADIUS to authenticate target credentials

This advanced settings page is the same as that of the discovery with one addition. On the ‘Connect using’ section the user can select the Target Port that he wishes to connect to. This is particularly useful if the user is going to create multiple connections. In this example we have chosen to connect to the IP-address 10.10.10.99 on port 3260.

Set up the Digest and CHAP settings as described in stage 2 during the discovery phase and click OK.

This will now take you back to the Connect to Target window. Click OK once more. The user should now see the iSCSI Target connected.



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Name	Status
iqn.2002-12.com.4bridgeworks.000000:977d098e36978...	Connected
iqn.2002-12.com.4bridgeworks.000000:977d0a8e36978...	Inactive

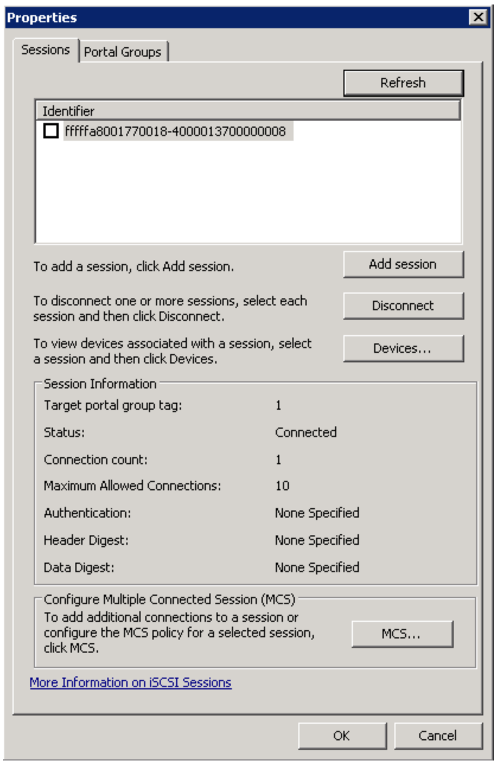
To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

Step 4 – Viewing iSCSI Session Details
Now that the user has connected to an iSCSI Target, to check that the device is connected click on the ‘Properties’ button. A window should appear.



□ ffffa8001770018-4000013700000008

To add a session, click Add session.

To disconnect one or more sessions, select each session and then click Disconnect.

To view devices associated with a session, select a session and then click Devices.

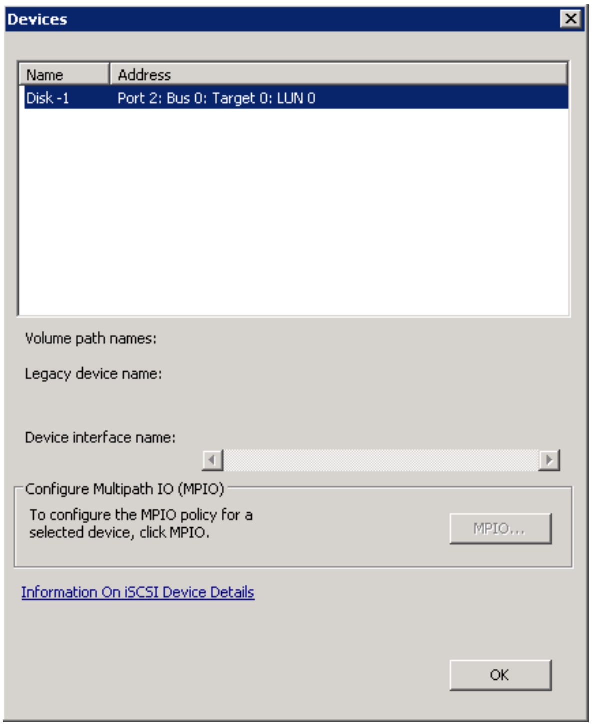
Session Information

Target portal group tag:	1
Status:	Connected
Connection count:	1
Maximum Allowed Connections:	10
Authentication:	None Specified
Header Digest:	None Specified
Data Digest:	None Specified

Configure Multiple Connected Session (MCS)
To add additional connections to a session or configure the MCS policy for a selected session, click MCS.

More Information on iSCSI Sessions

In this window the user can view the iSCSI Sessions associated to the iSCSI Target, how many connections are attached to each iSCSI Session, and the Target Portal Group. If the user clicks on the ‘Devices…’ tab, he should see details of the target device.



Name	Address
Disk -1	Port 2: Bus 0: Target 0: LUN 0

Volume path names:

Legacy device name:

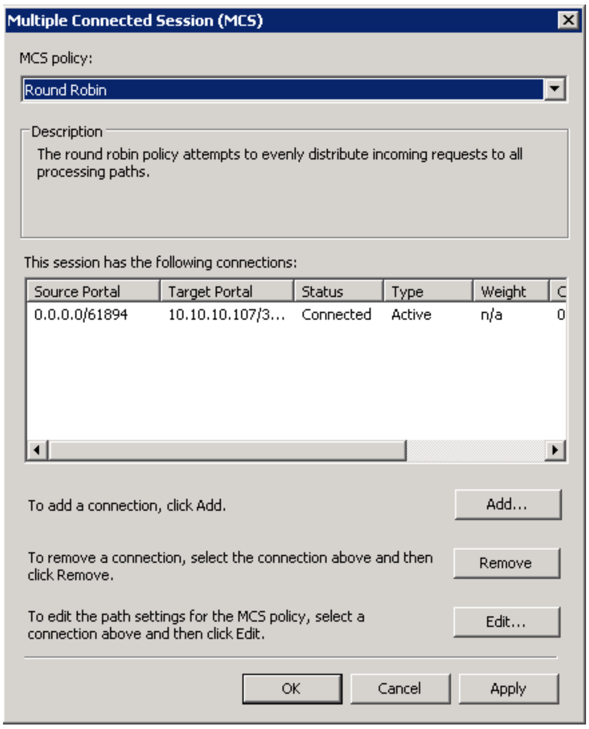
Device interface name:

Configure Multipath IO (MPIO)
To configure the MPIO policy for a selected device, click MPIO.

Information On iSCSI Device Details

Step 5 – Creating multiple connections (Optional)
If the user wishes to create multiple connections to an iSCSI Session, return to the Session tab in the Target Properties window.

Click on the ‘MCS…’ button and a window should appear. This is shown below.



Multiple Connected Session (MCS)

MCS policy:

Round Robin

Description

The round robin policy attempts to evenly distribute incoming requests to all processing paths.

This session has the following connections:

Source Portal	Target Portal	Status	Type	Weight	C
0.0.0.0/61894	10.10.10.107/3…	Connected	Active	n/a	0

To add a connection, click Add.

To remove a connection, select the connection above and then click Remove.

To edit the path settings for the MCS policy, select a connection above and then click Edit.

The Multiple Connected Session window shows how many iSCSI Connections are active and the type of load balance used. For all iSCSI Sessions there will be at least one ‘leading connection’.

iSCSI connections can be added and removed at any time, all apart from the leading connection, which can only be removed when the iSCSI Session is logged off.

The MCS policy specifies how the data is distributed over multiple connections. The main policies that should be used are ‘Round Robin’ and ‘Fail Over Only’.

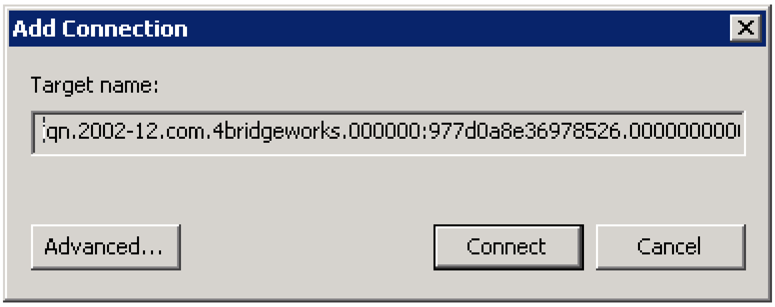
Round Robin will utilize all connections for data and evenly distribute the data.

Fail Over Only will use the Leading connection for data transfer. If a connection should go down then the data transfer shall switch on one of the other connections.

For most purposes Round Robin will provide the greatest performance increase.

If you have been experiencing a performance decrease when transferring data to more than one device using multiple connections, please refer to the trouble-shooting guide.

To add a new connection to a session, click on the Add button and a new window should appear.

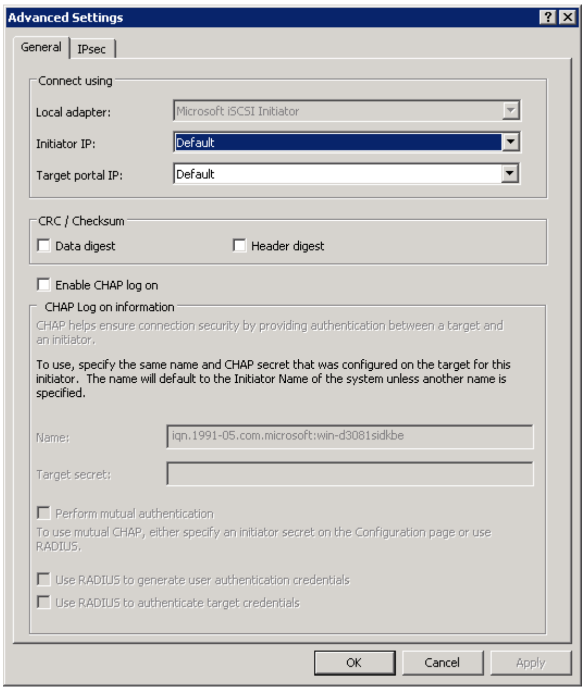


Add Connection

Target name:

qn.2002-12.com.4bridgeworks.000000:977d0a8e36978526.000000000

Now click on the ‘Advanced’ button to see the Advanced Settings.



Advanced Settings

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: Default

Target portal IP: Default

CRC / Checksum

□ Data digest □ Header digest

□ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:win-d3081sidkbe

Target secret:

□ Perform mutual authentication

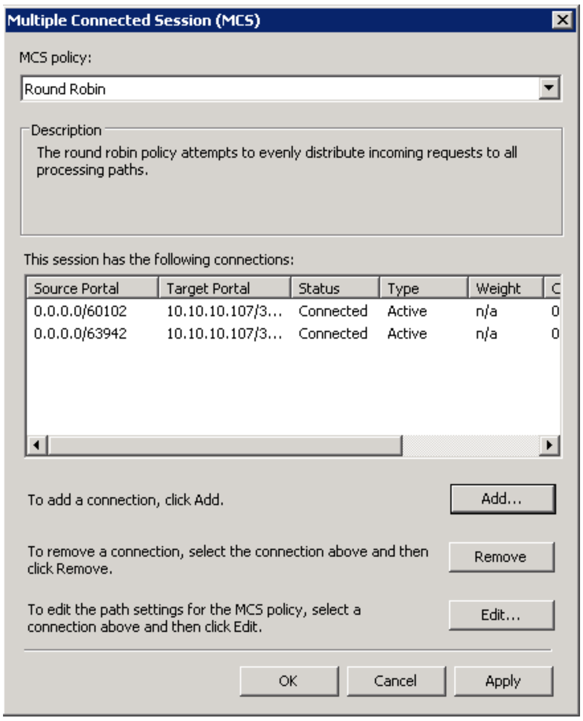
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

Select the Initiator IP-address and the Target Portal that you wish to connect too via the pull down menus in the “Connect by using” section. When setting up multiple connections you ideally want to connect to different ports and different network interfaces

Set up CHAP then click OK. The user will now be brought back to the window below. Click OK and now the user should see the Session Connections page with two connections.



Multiple Connected Session (MCS)

MCS policy: Round Robin

Description

The round robin policy attempts to evenly distribute incoming requests to all processing paths.

This session has the following connections:

Source Portal	Target Portal	Status	Type	Weight	C
0.0.0.0/60102	10.10.10.107/3...	Connected	Active	n/a	0
0.0.0.0/63942	10.10.10.107/3...	Connected	Active	n/a	0

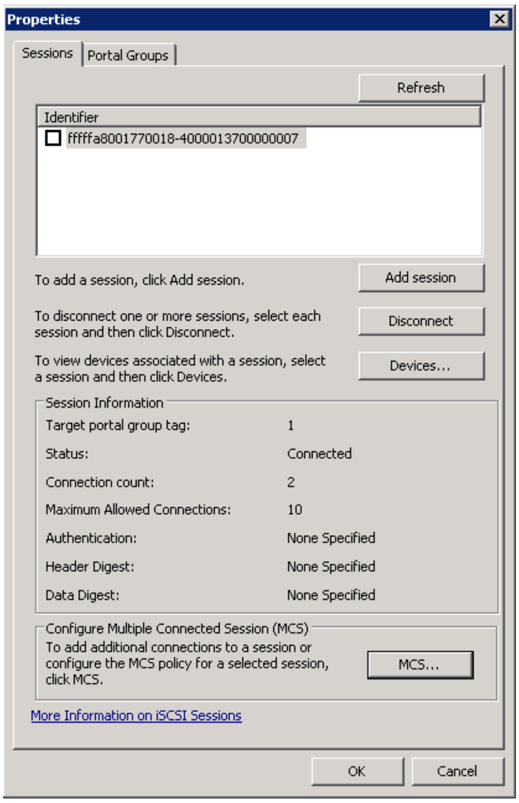
To add a connection, click Add.

To remove a connection, select the connection above and then click Remove.

To edit the path settings for the MCS policy, select a connection above and then click Edit.

The user can add up to 10 different connections.

Once the user has completed setting up the connections, click OK to return to the iSCSI session page. You should now see the number of connections increased. In this example we have 2 connections.



Identifier

□ ffffa8001770018-4000013700000007

To add a session, click Add session.

To disconnect one or more sessions, select each session and then click Disconnect.

To view devices associated with a session, select a session and then click Devices.

Session Information

Target portal group tag:	1
Status:	Connected
Connection count:	2
Maximum Allowed Connections:	10
Authentication:	None Specified
Header Digest:	None Specified
Data Digest:	None Specified

Configure Multiple Connected Session (MCS)

To add additional connections to a session or configure the MCS policy for a selected session, click MCS.

More Information on iSCSI Sessions

Now click on OK to return to the Microsoft iSCSI Initiator main window.

Step 6 – Logging off an iSCSI Session

To log off an iSCSI Session, follow the following procedure.

- Open the Microsoft iSCSI Initiator and click on the Targets tab.
- Click on the iSCSI session that the user wishes to log off.
- Click the ‘Disconnect’ button. This will log off all connections associated with the iSCSI Session.

The iSCSI device should now show as inactive.

Appendix C Removable Storage Service

The following only applies to Windows Server 2003.

You can use the Removable Storage service to temporarily disable an overflow of TUR requests. To do this, enable the service. Then, start and stop the service. This method stops the TUR requests until the computer is restarted or until the driver is changed.

Note: By default, the Removable Storage service is disabled.

To temporarily stop TUR requests, follow these steps:

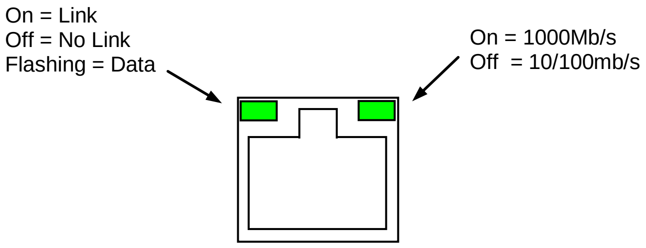
1. Click **Start**, type services.msc, and then click **OK**.
2. In the right pane, double-click **Removable Storage**.
3. In the **Startup type** list, click **Manual**, and then click **Apply**.
4. Click **Start**, and then click **Stop**.
5. In the **Startup type** list, click **Disabled**, and then click **OK**.

Further Information on this topic can be obtained from the Microsoft Website

http://support.microsoft.com/kb/842411

Appendix D LED Indicators

Ethernet



	Note: During heavy data transfers, the LED’s may appear off for an extended period.

Appendix E Technical Specifications

Physical	
Form Factor	19” 1U Rack mount
Depth	170mm (10.6 in)
Height	44mm (1.7 in)
Width	437mm (17.2 in)
Weight	5.1Kg
Recommended minimum clearance for cooling	100mm (4.in) on front and rear faces
Electrical	
Input voltage	110 –240V
Frequency	50 –60Hz
Input current	1 Amp Maximum
Maximum Power Consumption	60 Watts Maximum
Environmental	
Operating	0 to 40C (32F to 104F)
Non Operating	-20C to 60C (-4F to 140F)
Operating Humidity	5% to 90% Non-condensing
Storage Humidity	5% to 90% Non-condensing
Operating Altitude	3,000m (9,842ft)
Non Operating Altitude	8,000m (26,250ft)
iSCSI Interface	
Physical	RJ 45
Speed	10, 100, 1000Mb/s
Protocol	IPv4, CHAP, DHCP, NTP, iSNS
iSCSI Protocol	iSCSI RFC3270, 3721, ERL0, ERL1 ERL2
Visual Indicators	Link and Link activity